SpeedStream®

6500 Series

Residential Gateway User's Guide

Part No. 007-6770-001

© **Copyright 2004, Siemens Subscriber Network.**

All rights reserved. Printed in the U.S.A.

Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. Siemens Subscriber Networks shall not be liable for technical or editorial errors or omissions in this document; nor for incidental or consequential damages resulting from the furnishing, performance, or use of this material.

Siemens Subscriber Networks – End User Software License and Limited Warranty

INSTALLATION OF THE HARDWARE AND SOFTWARE PROVIDED BY SIEMENS SUBSCRIBER NETWORKS (SIEMENS) CONSTITUTES ACCEPTANCE BY YOU OF THE TERMS OF THE FOLLOWING SOFTWARE LICENSE AND LIMITED WARRANTY. IF YOU DO NOT ACCEPT THESE TERMS, PLEASE RETURN THE HARDWARE AND SOFTWARE IN ITS ORIGINAL PACKAGING TO THE STORE OR OTHER VENDOR FROM WHICH YOU PURCHASED IT FOR A FULL REFUND OF THE PURCHASE PRICE.

The following describes your license to use the software (the "Software") that has been provided with your SIEMENS DSL customer premises equipment ("Hardware") and the limited warranty that SIEMENS provides on its Software and Hardware.

Software License

The Software is protected by copyright laws and international copyright treaties. The Software is licensed and not sold to you. Accordingly, while you own the media (CD ROM or floppy disk) on which the Software is recorded, SIEMENS retains ownership of the Software itself.

1. **Grant of License**. You may install and use one (and only one) copy of the Software on the computer on which the Hardware is being installed. If the Hardware is being installed on a network, you may install the Software on the network server or other server-side device on which the Hardware is being installed and onto the client-side devices connected to the network as necessary.

2. **Restrictions**. The license granted is a limited license. You may NOT:

sublicense, assign, or distribute copies of the Software to others; decompile, reverse engineer, disassemble or otherwise reduce the Software or any part thereof to a human perceivable form; modify, adapt, translate or create derivative works based upon the Software or any part thereof; or rent, lease, loan or otherwise operate for profit the Software.

3. **Transfer**. You may transfer the Software only where you are also transferring the Hardware. In such cases, you must remove all copies of the Software from any devices onto which you have installed it, and must ensure that the party to whom you transfer the Hardware receives this License Agreement and Limited Warranty.

4. **Upgrades Covered**. This license covers the Software originally provided to you with the Hardware, and any additional software that you may receive from SIEMENS, whether delivered via tangible media (CD ROM or floppy disk), down loaded from SIEMENS or delivered through customer support. Any such additional software shall be considered "Software" for all purposes under this License.

5. **Export Law Assurance**. You acknowledge that the Software may be subject to export control laws and regulations of the U.S.A. You confirm that you will not export or re-export the Software to any countries that are subject to export restrictions.

6. **No Other Rights Granted**. Other than the limited license expressly granted herein, no license, whether express or implied, by estoppel or otherwise, is granted to any copyright, patent, trademark, trade secret, or other proprietary rights of SIEMENS.

7. **Termination**. Without limiting SIEMENS's other rights, SIEMENS may terminate this license if you fail to comply with any of these provisions. Upon termination, you must destroy the Software and all copies thereof.

Limited Warranty

The following limited warranties provided by SIEMENS extend to the original end user of the Hardware/licensee of the Software and are not assignable or transferable to any subsequent purchaser/licensee.

1. **Hardware**. SIEMENS warrants that the Hardware will be free from defects in materials and workmanship and will perform substantially in compliance with the user documentation relating to the Hardware for a period of one year from the date the original end user received the Hardware.

2. **Software**. SIEMENS warrants that the Software will perform substantially in compliance with the end user documentation provided with the Hardware and Software for a period of ninety days from the date the original end user received the Hardware and Software. The end user is responsible for the selection of hardware and software used in the end user's systems. Given the wide range of third-party hardware and applications, SIEMENS does not warrant the compatibility or uninterrupted or error free operation of our Software with the end user's system.

3. **Exclusive Remedy**. Your exclusive remedy and SIEMENS's exclusive obligation for breach of this limited warranty is, in SIEMENS's sole option, either (a) a refund of the purchase price paid for the Hardware/Software or (b) repair or replacement of the Hardware/Software with new or remanufactured products. Any replacement Hardware or Software will be warranted for the remainder of the original warranty period or thirty (30) days, which ever is longer.

4. **Warranty Procedures**. If a problem develops during the limited warranty period, the end user shall follow the procedure outlined below:

A. Prior to returning a product under this warranty, the end user must first call SIEMENS at (888) 286-9375, or send an email to SIEMENS at support@efficient.com to obtain a return materials authorization (RMA) number. RMAs are issued between 8:00 a.m. and 5:00 p.m. Central Time, excluding weekends and holidays. The end user must provide the serial number(s) of the products in order to obtain an RMA.

B. After receiving an RMA, the end user shall ship the product, including power supplies and cable, where applicable, freight or postage prepaid and insured, to SIEMENS at 4849 Alpha Road, Dallas Texas 75244, U.S.A. Within five (5) days notice from SIEMENS, the end user shall provide SIEMENS with any missing items or, at SIEMENS's sole option, SIEMENS will either (a) replace missing items and charge the end user or (b) return the product to the end user freight collect. The end user shall include a return address, daytime telephone number and/or fax. The RMA number must be clearly marked on the outside of the package.

C. Returned Products will be tested upon receipt by SIEMENS. Products that pass all functional tests will be returned to the end user.

D. SIEMENS will return the repaired or replacement Product to the end user at the address provided by the end user at SIEMENS's expense. For Products shipped within the United States of America, SIEMENS will use reasonable efforts to ensure delivery within five (5) business days from the date received by SIEMENS. Expedited service is available at additional cost to the end user.

E. Upon request from SIEMENS, the end user must prove the date of the original purchase of the product by a dated bill of sale or dated itemized receipt.

5.**Limitations**.

The end user shall have no coverage or benefits under this limited warranty if the product has been subject to abnormal use, abnormal conditions, improper storage, exposure to moisture or dampness, unauthorized modifications, unauthorized repair, misuse, neglect, abuse, accident, alteration, improper installation, or other acts which are not the fault of SIEMENS, including acts of nature and damage caused by shipping.

SIEMENS will not honor, and will consider the warranty voided, if: (1) the seal or serial number on the Product have been tampered with; (2) the Product's case has been opened; or (3) there has been any attempted or actual repair or modification of the Product by anyone other than an SIEMENS authorized service provider.

The limited warranty does not cover defects in appearance, cosmetic, decorative or structural items, including framing, and any non-operative parts.

SIEMENS's limit of liability under the limited warranty shall be the actual cash value of the product at the time the end user returns the product for repair, determined by the price paid by the end user for the product less a reasonable amount for usage. SIEMENS shall not be liable for any other losses or damages.

The end user will be billed for any parts or labor charges not covered by this limited warranty. The end user will be responsible for any expenses related to reinstallation of the product.

THIS LIMITED WARRANTY IS THE ONLY WARRANTY SIEMENS MAKES FOR THE PRODUCT AND SOFTWARE. TO THE EXTENT ALLOWED BY LAW, NO OTHER WARRANTY APPLIES, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

6. **Out of Warranty Repair**. Out of warranty repair is available for fixed fee. Please contact SIEMENS at the numbers provided above to determine the current out of warranty repair rate. End users seeking out of warranty repair should contact SIEMENS as described above to obtain an RMA and to arrange for payment of the repair charge. All shipping charges will be billed to the end user.

General Provisions

The following general provisions apply to the foregoing Software License and Limited Warranty:

1. **No Modification**. The foregoing limited warranty is the end user's sole and exclusive remedy and is in lieu of all other warranties, express or implied. No oral or written information or advice given by SIEMENS or its dealers, distributors, employees or agents shall in any way extend, modify or add to the foregoing Software License and Limited Warranty. This Software License and Limited Warranty constitutes the entire agreement between SIEMENS and the end user, and supersedes all prior and contemporaneous representation, agreements or understandings, oral or written. This Software License and Limited Warranty may not be changed or amended except by a written instrument executed by a duly authorized officer of SIEMENS.

SIEMENS neither assumes nor authorizes any authorized service center or any other person or entity to assume for it any other obligation or liability beyond that which is expressly provided for in this limited warranty including the provider or seller of any extended warranty or service agreement.

The limited warranty period for SIEMENS supplied attachments and accessories is specifically defined within their own warranty cards and packaging.

2. **EXCLUSION OF INCIDENTAL, CONSEQUENTIAL AND CERTAIN OTHER DAMAGES**. TO THE FULL EXTENT PERMITTED BY LAW, IN NO EVENT SHALL SIEMENS BE LIABLE, WHETHER UNDER CONTRACT, WARRANTY, TORT OR ANY OTHER THEORY OF LAW FOR ANY SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES WHATSOEVER, INCLUDING BUT NOT LIMITED TO DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION, PERSONAL INJURY, LOSS OR IMPAIRMENT OF DATA OR BUSINESS INFORMATION, EVEN IF SIEMENS HAS BEEN NOTIFIED OF THE POSSIBILITY OF SUCH DAMAGES. SIEMENS'S LIABILITY TO YOU (IF ANY) FOR ACTUAL DIRECT DAMAGES FOR ANY CAUSE WHATSOEVER, AND REGARDLESS OF THE FORM OF THE ACTION, WILL BE LIMITED TO, AND SHALL NOT EXCEED, THE AMOUNT PAID FOR THE HARDWARE/SOFTWARE.

3. **General**. This Software License and Limited Warranty will be covered by and construed in accordance with the laws of the State of Texas, United States (excluding conflicts of laws rules), and shall inure to the benefit of SIEMENS and its successor, assignees and legal representatives. If any provision of this Software License and Limited Warranty is held by a court of competent jurisdiction to be invalid or unenforceable to any extent under applicable law, that provision will be enforced to the maximum extent permissible, and the remaining provisions of this Software License and Limited Warranty will remain in full force and effect. Any notices or other communications to be sent to SIEMENS must be mailed by certified mail to the following address:

Siemens Subscriber Networks

4849 Alpha Road

Dallas, TX 75244

U.S.A.

Attn: Customer Service

Contents

CHAPTER 1 INTRODUCTION 1

Features of the Residential Gateway Family 1
Network (LAN) Features 1
Security Features 1
Configuration & Management 2
Advanced Gateway Functions 2
Minimum System Requirements 3
USB Driver-Related Requirements 3
Package Contents 3
Physical Details 4
Front Panel LEDs 4
Rear Panel 5
General Safety Guidelines 5

CHAPTER 2 INSTALLATION 6

Minimum System Requirements 6
Hardware Installation 6
Basic Installation Procedure 6
Installing Line Filters 7
Connecting Cables 8

CHAPTER 3 10

OPERATING SYSTEM CONFIGURATION 10

Check TCP/IP Protocol Settings 10
Checking TCP/IP Settings (Windows 9x/ME) 11
Checking TCP/IP Settings (Windows 2000) 12
Checking TCP/IP Settings (Windows XP) 13
Checking TCP/IP Settings (MAC OS 8.6 through 9.x) 14
Checking TCP/IP Settings (MAC OSX) 15
Internet Access Configuration 16
For Windows 9x/2000 16
For Windows XP 16

CHAPTER 4 SPEEDSTREAM GATEWAY SETUP 17

Before Configuring the Gateway 17
Connecting to the Gateway 18
Gateway Setup Wizard 19
Home Window 26
Menu Bar 26
Toolbar 27
Logging into the Gateway 27
Logging out of the Gateway 27

CHAPTER 5 CONFIGURING USERS AND DEVICES 28

Configuring Users 28
Adding a User 28
Editing A User Profile 33
Deleting a User 34
Viewing User Logs 35
Configuring Devices 36

CHAPTER 6 CONFIGURING ADVANCED FEATURES 37

ISP Connection 38
Advanced ISP Settings 39
ATM Virtual Circuits 40
Static Routes 41
Dynamic DNS 42
RIP (Routing Information Protocol) 43
Home Network 44
IP Network 45
Server Ports 46
LAN/WAN Port 47
Wireless Network 48
Powerline Security Configuration 55
UPnP (Universal Plug and Play) 57
Security 59
Firewall Settings 60
Administrator Password 72
Address Translation 73

CHAPTER 7 MONITORING GATEWAY HEALTH 77

Statistics 78
Update Firmware 82
Diagnostics 83

CHAPTER 8 MISCELLANEOUS GATEWAY OPTIONS 84

Customize 84
Color Palette 85
Language 86
Time Zone 87
Reboot 88

APPENDIX A TROUBLESHOOTING 89

Overview 89
General Issues 89
Internet Access 89
Contacting Technical Support 90

APPENDIX B SPECIFICATIONS 91

Chapter 1

Introduction

This chapter provides an overview of the Gateway's features and capabilities.

Congratulations on the purchase of your new SpeedStream SS6500 Series Residential Gateway (Gateway). The Gateway is a multi-function device providing the following services:

- Built-in DSL Modem that provides shared Internet access for multiple users.
- One- or four-port 10/100 Ethernet Switch for 10Base-T or 100Base-T connections.
- Custom Controls that allow you to configure the SpeedStream Residential Gateway to best meet your specific security and Internet-sharing needs.
- Integrated 802.11g/802.11b wireless interface that provides a wireless interface built into the unit.

Features of the Residential Gateway

The SpeedStream SS6500 Series Gateway incorporates many advanced features, carefully designed to provide sophisticated functions while being easy to use.

Network (LAN) Features

- **One- or Four-Port 10/100 Ethernet Switch**
  The SpeedStream Gateway incorporates a one- or four-port 10/100 Ethernet switch, making it easy to create or extend your network. Optionally, you can configure the fourth port as a WAN port for connection to another broadband device.
- **DHCP Server Support**
  Dynamic Host Configuration Protocol (DHCP) provides a dynamic, “upon request,” IP address to computers and other networked devices. Your SpeedStream Gateway can act as a DHCP Server for devices on your local network.
- **Network Status and Statistics**
  Using these diagnostic tools, you can easily monitor the status of each network connection and evaluate network performance.
- **USB Connection**
  Some Gateways will have a Universal Serial Bus (USB) connection that can be used to connect up to 127 peripheral devices, such as mice, modems, and keyboards. It also supports UPnP installation and hot plugging.

Security Features

- **Password Protected Configuration**
  Password protection is provided to prevent unauthorized users from modifying the Gateway’s configuration data and settings.
- **NAT Protection**
  An intrinsic side affect of NAT (Network Address Translation) technology is that by allowing all your network users to share a single IP address, the location and even the existence of each computer is hidden. From the external viewpoint, there is no network, only a single device - the SpeedStream Gateway.

- **Stateful Inspection Firewall**
  All incoming data packets are monitored and all incoming server requests are filtered, thus protecting your network from malicious attacks from external sources.
- **Attack Protection System**
  Attacks can flood your Internet connection with invalid data packets and connection requests, using so much bandwidth and so many resources that Internet access becomes unavailable. The Gateway incorporates protection against these types of attacks as well as other common hacker attacks.

Configuration & Management

- **Easy Setup**
  Use your Web browser for quick and easy configuration.
- **UPnP Support**
  Universal Plug and Play (UPnP) allows automatic discovery and configuration of the SpeedStream Gateway. UPnP is supported by Windows Me, XP or later, operating systems.

Advanced Gateway Functions

- **DMZ**
  One computer on your local network can be configured to allow unrestricted two-way communication with servers or individual users on the Internet. This provides the ability to run programs that are incompatible with firewalls.
- **Firewall "Snooze**"
  Temporarily disable firewall protection to limit interference with games and other applications incompatible with firewalls.
- **Content Filter**
  Use the Content Filter to block individual user access to undesirable Web sites. Content filtering can be defined differently for each user.
- **Time of Day Use Restrictions**
  Limit the time of day during which individual users have access to the Internet. Time limitations can be defined differently for each user.
- **Advanced Wireless Controls**
  The SpeedStream 6500 model has a built-in wireless interface. Custom configuration options include wireless access control, 64-bit, 128-bit, or WAP wireless encryption, disable SSID broadcast, and pass phrase key generation for added security.
- **HPNA**
  Some Gateways will come with Home Phoneline Networking Alliance (HPNA). HPNA technology, building on Ethernets, allows all the components of a home network to interact over the home's existing telephone wiring without disturbing the existing voice or fax services.
- **Powerline**
  Some Gateways will come with Digital Powerline (DPL) capability. DPL technology provides the transmission of data to users over the same lines that bring electric power to homes and businesses using TCP/IP protocol.

Minimum System Requirements

At a minimum, your computer must be equipped with the following to successfully install the Gateway. Your Internet Service Provider may have additional requirements for use of their service.

- **Ethernet connection method**
  - A network interface card (NIC) that supports 10/100 Ethernet
  - Operating system that supports TCP/IP
  - Microsoft Internet Explorer or Netscape Navigator versions 5.0 or later
- **USB connection method**
  - Available built-in USB port
  - Microsoft Internet Explorer or Netscape Navigator versions 5.0 or later

USB Driver-Related Requirements

Additional USB driver-related requirements depend on the operating system and architecture:

- **Windows operating system**
  - Pentium-compatible 166 MHz (or faster) processor
  - 32 MB RAM
  - 10 MB available hard drive space
  - Windows 98 or later operating system
- **Macintosh operating system version 8.6 to 10.2.4**
  - 100MHz PowerPC or better
  - 32 MB RAM
  - 10 MB available hard disk space
- **Macintosh operating system X**
  - 300MHz PowerPC G3 or better
  - 128 MB RAM
  - 110 MB available hard disk space (large space requirement due to the Macintosh OS X needing up to 100 MB of additional disk space for system organization after install)

Package Contents

If any of the items are damaged or missing, please contact your Internet Service Provider for assistance.

- Model SS6500 Series SpeedStream Residential Gateway
- Power adapter
- CAT-5 Ethernet cable for LAN connections
- RJ11 cable for DSL connection
- USB cable for optional USB installation (on some models)
- Quick Start Guide
- CD-ROM containing USB driver software and user documentation (on some models)

Physical Details

Familiarize yourself with the Gateway before installing.

Front Panel LEDs

The front panel contains the following LEDs:

Power	**Green**	Power is on.
	Off	Power is off.
	Red	The Power LED briefly shows red during power-up. This indicates that the SpeedStream is conducting the POST (Power-On Self Test) that is run each time the SpeedStream is powered on.
Ethernet	**On**	One or more Ethernet LAN ports are active.
	Off	No active Ethernet LAN port connection.
Wireless	**On**	Wireless connection is active.
	Off	No active wireless connection.
DSL	**On**	DSL connection is active.
	Off	No active DSL connection.
Internet	**Green**	Internet connection has been established.
Activity (if present)	**Off**	No data being transmitted or received.
	Flashing	Data is being transmitted or received.
USB (if present)	**On**	USB connection is active.
	Off	No active USB connection.
HPNA (if present)	**On**	HPNA connection is active.
	Off	No active HPNA connection.
HomePlug (if present)	**On**	Powerline connection is active.
	Off	No active powerline connection.

Example Front Panel

Rear Panel

DSL Port (RJ11)	Connect the RJ11 DSL cable (looks like a telephone cord) here to use your DSL connection through an existing phone line.
USB Port	If your Gateway has a USB port, connect the USB cable here. The USB driver software must be installed from the provided CD-ROM.
10/100 Ethernet Ports 1 - 4	Connect the RJ45 Ethernet cable here to connect your computers, hubs, or switches to the Gateway. If your model has four ports, you can configure port #4 as either a LAN or WAN port.
Power Adapter Port	Connect the supplied power adapter provided with the Gateway here.
Power Button	Push this button to power the Gateway on and off.

Example Rear Panel

General Safety Guidelines

When using the SpeedStream Gateway, observe the following safety guidelines:

- Never install telephone wiring during a storm.
- Avoid using a telephone during an electrical storm. Lightening increases the risk of electrical shock.
- Do not install telephone jacks in wet locations and never use the product near water.
- Do not exceed the maximum power load ratings for the product; otherwise, you risk dangerous overloading of the power circuit.

Chapter 2

Installation

This chapter covers the physical installation of the SpeedStream Gateway.

Minimum System Requirements

- DSL service and an Internet access account from an Internet Service Provider (ISP).
- Network cables for each device you intend to connect to the Gateway.
- TCP/IP network protocol must be installed on all computers.
- For USB connection to the Gateway, the following operating systems are supported:
  - Windows 98, 98SE
  - Windows 2000
  - Windows ME or XP
  - Mac OS versions 8.6 through 10.2.4

Note: Your configuration may vary slightly from the instructions and illustrations in this chapter. Refer to your service provider's documentation, or contact them with questions regarding your specific configuration.

Hardware Installation

You may position the SpeedStream Gateway at any convenient location in your office or home. No special wiring or cooling requirements are needed; however, you should comply with the safety guidelines specified in the General Safety Guidelines section.

Basic Installation Procedure

1. Install line filters if necessary.
2. Connect the cables.
3. Install USB drivers if necessary.
4. Configure network settings on your computer.
5. Configure the Gateway via the Web-based management interface.
6. Reboot the computer if prompted. Whenever you are required to reboot the Gateway, allow five seconds between turning off the unit and powering it back on.

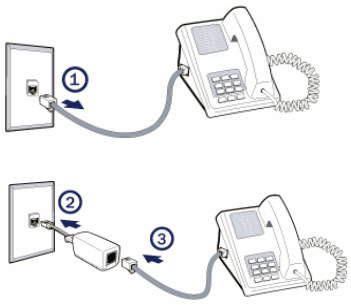
Installing Line Filters

Because DSL shares your telephone line, you may need to separate the two signals so they do not interfere with each other. A line filter (may be included with some models) prevents DSL traffic from disrupting the voice signal on the telephone line, and vice versa. Follow the procedures below to install line filters on any device (telephones, fax machines, caller ID boxes) that shares the same telephone line with your DSL. (Note, this section may not apply to you. Consult your provider if you are unsure.)

There are two types of filters to connect between the telephone and the wall plate:

- *In-line filter:* For use with standard desktop telephones.
- *Wall-mount filter*: For use with wall-mounted telephones.

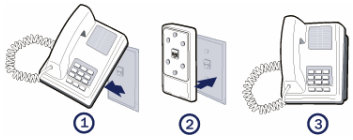
DSL performance may be significantly degraded if the line filters are not installed in the correct direction, as illustrated below.



In-Line Filter

For each device sharing the same telephone line:

1. Unplug the device's cord from the telephone jack.
2. Plug the filter into the telephone jack.
3. Plug the telephone cord (or other device cord) into the filter.



Wall-Mount Filter

For a wall-mounted telephone, install a wall mount filter:

1. Remove the telephone.
2. Connect the wall mount filter to the wall plate.
3. Reconnect the telephone.

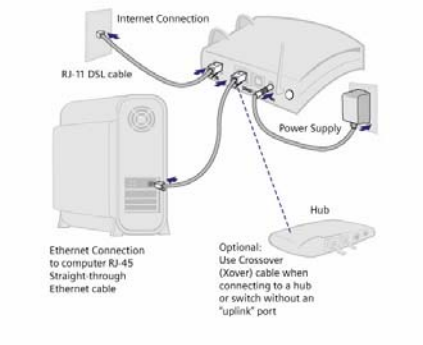
Connecting Cables

The SpeedStream Gateway provides ports for either a USB or an Ethernet connection to your primary computer. Select the interface you will use to connect the Gateway, and follow the step-by-step instructions below for your chosen installation method.

Ethernet Installation Method

To connect the SpeedStream Gateway via the Ethernet interface, your computer must have an Ethernet adapter (also called a network interface card, or "NIC") installed.

If your computer does not have this adapter, install it before proceeding further. Refer to your Ethernet adapter documentation for complete installation instructions.


Internet Connection
RJ-11 DSL cable
Power Supply
Hub
Ethernet Connection to computer RJ-45 Straight-through Ethernet cable
Optional: Use Crossover (Xover) cable when connecting to a hub or switch without an "uplink" port

1. Connect the Ethernet cable(s)

1) With your computer powered off, connect the Ethernet cable to an Ethernet port (1-4) on the Gateway.
2) Connect the other end of the Ethernet cable to the Ethernet port on your computer.
3) If desired, use standard 10/100 CAT5 Ethernet cables to connect additional computers to the remaining Ethernet ports on the Gateway.

2. Connect the DSL cable

1) Connect the DSL cable (resembles a telephone cord) to the DSL port on the Gateway.
2) Plug the other end of the DSL cable into the phone jack.

3. Connect the power

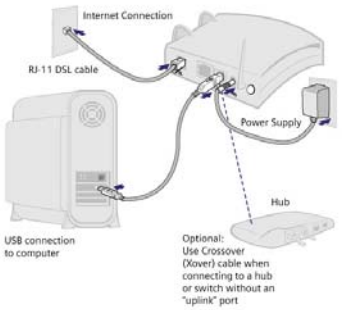
1) Connect the power adapter to the rear of the Gateway.
2) Plug the power adapter into the electrical wall outlet.
3) Flip the power switch to power on the SpeedStream Gateway.
4) Power on all connected computers.

4. Check the LEDs

1) For each active Ethernet connection, the LAN Link LED for the corresponding port number should be lit.
2) The DSL and Power LEDs should be lit. (For more information, refer to the LEDs section in Chapter 1.)

When using the Ethernet installation method, you do not have to install any software. Refer to your Internet Service Provider's instructions for installing their software and/or connecting to the Internet. You can now configure the TCP/IP settings as detailed in the next chapter.

USB Installation Method (Microsoft Windows)


Internet Connection
RJ-11 DSL cable
Power Supply
Hub
USB connection to computer
Optional: Use Crossover (Xover) cable when connecting to a hub or switch without an "uplink" port

1. Connect the USB Cable

1) With your computer off, connect the provided USB cable to the USB port on the Gateway.

2) Connect the other end of the USB cable to an open USB port on your computer.

3) If desired, use standard 10/100 CAT5 Ethernet cables to connect additional computers to the Ethernet ports on the Gateway.

2. Connect the DSL Cable

1) Connect the DSL cable (resembles a telephone cord) to the DSL port on the Gateway.

2) Plug the other end of the DSL cable into the phone jack.

3. Connect the Power

1) Connect the power adapter to the rear of the Gateway.

2) Plug the power adapter into the electrical wall outlet.

3) Flip the power switch to power on the Gateway.

4) Power on all connected computers.

4. Install USB Driver Software

1) Insert the USB driver CD-ROM into the CD-ROM drive of your computer.

2) When prompted, follow the on-screen instructions to complete the driver installation.

5. Check the LEDs

1) The DSL, USB, and Power LEDs should be lit. (For more information, refer to the LEDs section in Chapter 1.)

You can now configure the TCP/IP settings as detailed in the next chapter.

USB Driver Installation (Macintosh Systems)

When using the USB installation method on a Macintosh, follow these steps to install the USB drivers:

1. Insert the SpeedStream Installation CD into your CD-Rom drive.
2. Open the SpeedStream icon from the desktop.
3. Click Readme.txt to open it.
4. Follow the directions in the Readme.txt file.

You can now configure the TCP/IP settings as detailed in the next chapter.

Chapter 3

Operating System Configuration

This chapter explains how to configure each computer on your network to work with the Gateway.

To access the Internet through the SpeedStream Gateway, the TCP/IP protocol must be installed on your computer. If TCP/IP is not already installed on your computer, install it. Refer to your system documentation or online help for instructions.

- Once TCP/IP is installed on your computer, you should check the TCP/IP protocol settings to make sure they are correct for use with the Gateway.
- Once TCP/IP configuration is verified, the next step is to configure your computer to use the Gateway for internet access so your PC will use the Gateway when connecting to the Internet and not Dial-Up Networking.

The operating system on each computer in your network must have the TCP/IP network settings and Internet access settings configured.

Check TCP/IP Protocol Settings

Because the Gateway uses the TCP/IP network protocol for all functions, it is essential that the TCP/IP protocol be installed and configured properly.

The default network settings for the SpeedStream Gateway are:

IP Address:	192.168.254.254
Subnet Mask:	255.255.255.0

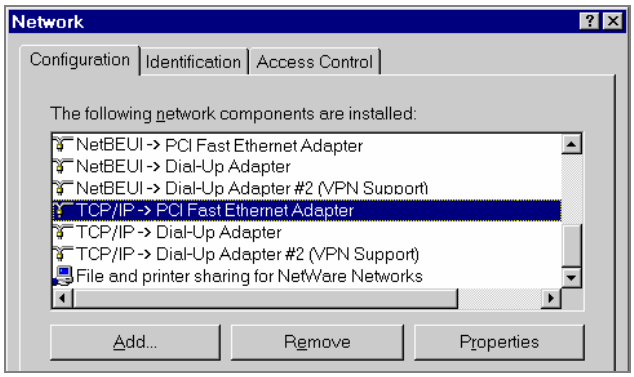
By default, the Gateway will act as a DHCP server, automatically providing a suitable IP address and related information to each computer when the computer boots up. For all non-server versions of Windows, the TCP/IP setting defaults to act as a DHCP client. If using the default Gateway settings and the default Windows TCP/IP settings, you do not need to make any changes.

The instructions to check TCP/IP protocol settings differ between operating system. Check the settings using the instructions for your operating system:

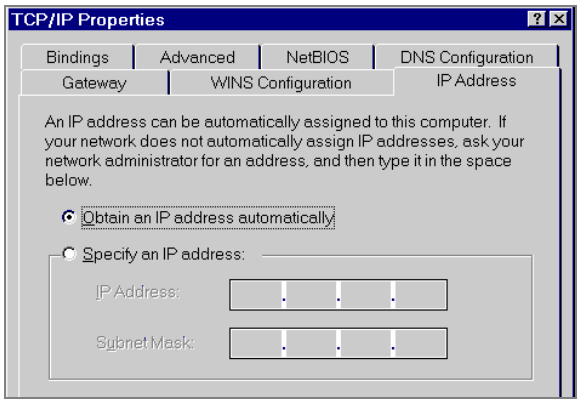
- Windows 9x/ME
- Windows 2000
- Windows XP
- MAC OS 8.6 through 9.x
- MAC OSX

Checking TCP/IP Settings (Windows 9x/ME)

1. Select **Start>Control Panel >Network**. This displays the **Configuration** tab on the "Network" window.



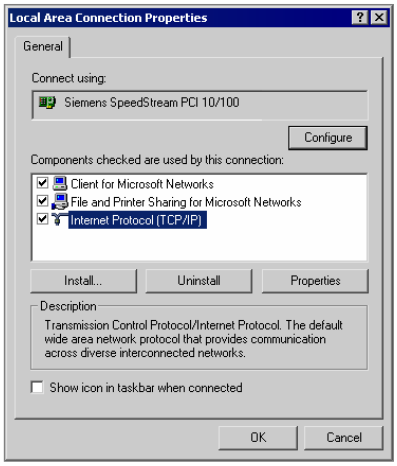
2. Select the TCP/IP protocol for your network card.
3. Click **Properties**. This displays the "TCP/IP Properties" window.

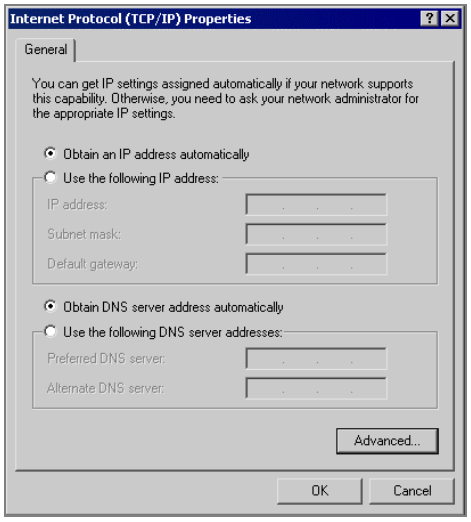

TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:

4. Click the **IP Address** tab.
5. Ensure that the **Obtain an IP address automatically** option is selected. This is the default Windows settings.
6. Close this window.
7. Restart your computer to ensure it obtains an IP address from the Gateway.
8. Configure internet access using the procedure described in Internet Access Configuration.

Checking TCP/IP Settings (Windows 2000)

1. On the Windows taskbar click **Start>Settings>Control Panel**. This displays the "Control Panel" window.
2. Double-click **Network and Dial-up Connections**. This displays the "Network and Dial-up Connections" window.
3. Right-click **Local Area Connection** and select Properties. This displays the "Local Area Connections Properties" window.
4. Select the TCP/IP protocol for your network card.
5. Click **Properties**. This displays the "Internet Protocol (TCP/IP) Properties" window.

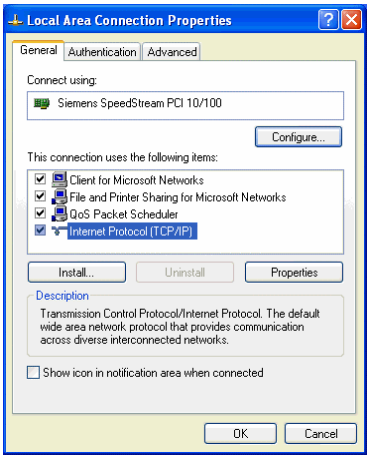


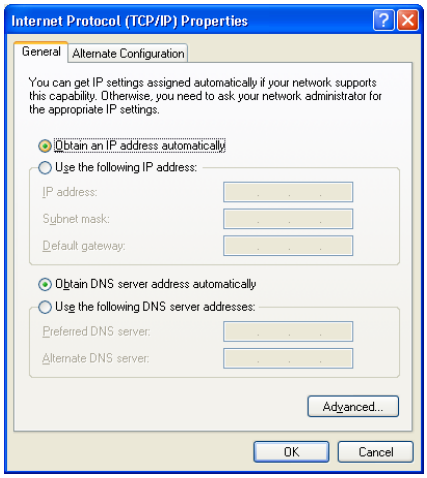

Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

6. Select the **Obtain an IP address automatically** and **Obtain DNS server address automatically** options. Exit back to the Control Panel.
7. Restart your computer to ensure it obtains an IP address from the Gateway.
8. Configure internet access using the procedure described in Internet Access Configuration.

Checking TCP/IP Settings (Windows XP)

1. On the Windows taskbar click **Start>Control Panel**. This displays the "Control Panel" window.
2. Double-click the **Network Connection** icon. This displays the "Network Connections" window.
3. Right-click **Local Area Connection**, then click **Properties**. This displays the "Local Area Connection Properties" window.
4. Select the TCP/IP protocol for your network card.
5. Click **Properties**. This displays the "Internet Protocol (TCP/IP) Properties" window.

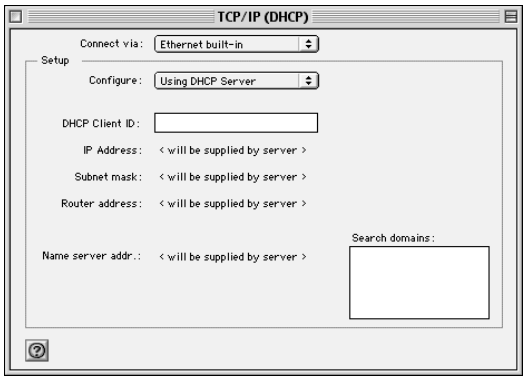



Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

6. Ensure that **Obtain an IP address automatically** and **Obtain DNS server address automatically** are selected.
7. Exit back to the Control Panel.
8. Restart the computer to ensure it obtains an IP address from the Gateway.
9. Configure internet access using the procedure described in Internet Access Configuration.

Checking TCP/IP Settings (MAC OS 8.6 through 9.x)

1. Select **Apple >Control Panel >TCP/IP**. This displays the "TCP/IP" window.



2. Select one of the following from the **Connect via** drop-down menu.
   - **Ethernet** or **Ethernet built-in** if connecting via Ethernet.
   - **Ethernet Adaptor [en0,en1,…]** if connecting via USB.
3. Select **Using DHCP Server** from the **Configure** drop-down menu.
4. Close the "TCP/IP window" and click **Save**.
5. Reboot when configuration is saved. Once rebooted, the computer will pull an IP address from the DHCP server on the Gateway.
6. Configure the Gateway using the procedure described in the next chapter.

Checking TCP/IP Settings (MAC OSX)

1. Click **Apple -> System Preferences**. This displays the "System Preferences" window.

2. Double-click the **Network** icon under the **Internet & Network** section. This displays the "Network" window.

3. Select one of the following from the **Show** drop-down menu:
   - **Built-in Ethernet** if connecting via Ethernet.
   - **Ethernet Adaptor [en0,en1,…]** if connecting via USB.
4. Select **Using DHCP Server** from the **Configure IPv4** drop-down menu.
5. Click **Apply Now** and quit window.
6. Configure the Gateway using the procedure described in the next chapter.

Internet Access Configuration

Windows users must configure their computers to use the Gateway for Internet access. Ensure that the Gateway is installed correctly and the DSL line is functional. Then follow the appropriate procedure below to configure your Web browser to access the Internet via the LAN, rather than by a dial-up connection.

For Windows 9x/2000

1. Select **Start>Settings>Control Panel** to display the Control Panel.
2. Double-click the **Internet Options** icon. This displays the "Internet Properties" window.
3. Click the **Connections** tab.
4. Click **Setup**.
5. Click **I want to set up my Internet connection manually**, or **I want to connect through a local area network (LAN)**, then click **Next**. This displays the "Internet Connection Wizard" window.
6. Click **I connect through a local area network (LAN)**, then click **Next**. This displays the "Local Area Network Internet Configuration" window.
7. Ensure all the boxes are deselected, then click **Next**. This displays the "Set Up your Internet Mail Account" window.
8. Click **No**, then click **Next**. This displays the "Completing the Internet Connection Wizard" window.
9. Click **Finish** to close the Internet Connection Wizard. Setup is now complete.
10. Configure the Gateway using the procedure described in the next chapter.

For Windows XP

1. Select **Start>Control Panel**.
2. Double-click the **Internet Options** icon. This displays the "Internet Options" window.
3. Click the **Connections** tab.
4. Click **Setup**. This starts the **New Connection Wizard**.
5. Click **Next**.
6. Select **Connect to the Internet**, then click **Next**.
7. Select **Setup my connection manually**, then click **Next**.
8. Select **Connect using a broadband connection that is always on**, then click **Next**.
9. Click **Finish**.
10. Configure the Gateway using the procedure described in the next chapter.

Chapter 4

SpeedStream Gateway Setup

This chapter describes how to connect to and setup your Gateway configuration.

This chapter describes the steps to set up the SpeedStream Gateway configuration using the Gateway Setup Wizard. Other configuration may also be required on the Gateway, depending on which features and functions of the Gateway you wish to use. Use the table below to locate detailed instructions for the required functions.

To do this	Refer to
Configure users and devices on the Gateway.	Chapter 5, Configuring Users and Devices
Configure Gateway advance options such as ISP connections, networking options, and security.	Chapter 6, Configuring Advanced Features
Monitor the health of the Gateway.	Chapter 7, Monitoring Gateway Health

Before Configuring the Gateway

Before attempting to configure the Gateway, please ensure that:

- Your computer can establish a physical connection to the Gateway. The computer and the Gateway must be directly connected using either the USB or Ethernet ports on the Gateway.
- The SpeedStream Gateway is installed correctly and powered on.
- The TCP/IP protocol is installed on all computers on your network. (If you need to install TCP/IP, refer to your system documentation or Windows Help.)
- The network settings on each computer are correctly configured.

From this point on, you will perform all configuration of the Gateway from your computer using the Web browser-based setup program.

Connecting to the Gateway

You can connect to the Gateway using UPnP (if it is enabled on your computer) or through the Web browser.

Using UPnP (Windows XP and Me)

If your Windows operating system supports UPnP (Universal Plug and Play) and UPnP is enabled, an icon for the Gateway appears in the system tray near the time display, notifying you that a new network device has been found and offering to create a new desktop shortcut to the newly discovered device.

Note: You must be logged in as administrator or be a user with administrative rights for Windows 2000 and XP to be able to install the drivers for the Gateway.

1. Unless you intend to change the IP address of the Gateway, you can accept the desktop shortcut. Whether you accept the desktop shortcut or not, you can find UPnP devices in **My Network Places** (previously called Network Neighborhood).
2. Double-click the icon for the Gateway (either on the desktop or in **My Network Places**) to access the Gateway's configuration program.
3. Refer to the Setup Wizard section for details of the initial configuration process.

Using your Web Browser

The SpeedStream Gateway contains an HTTP server that allows you to connect to the Gateway and configure it from your Web browser (Microsoft Internet Explorer or Netscape Navigator, versions 5.0 or later).

To establish a connection from your computer to the Gateway:

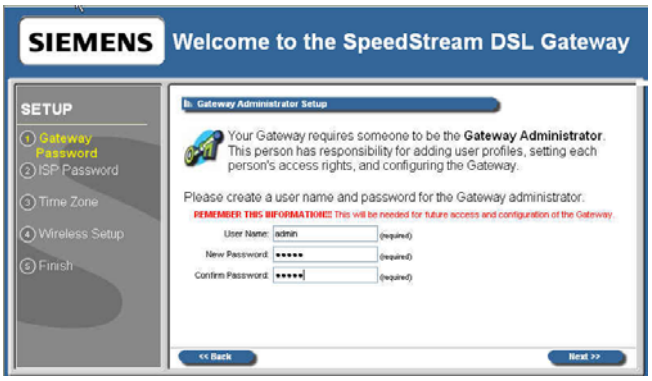
1. After installing the Gateway, start your computer. If your computer is already running, reboot it.
2. Open your Internet Explorer or Netscape Navigator Web browser.
3. In the **Address** bar, type **http://speedstream** and press the **Enter** key. This displays the "Setup" window.
4. Refer to the Setup Wizard section for details of the initial configuration process.

Gateway Setup Wizard

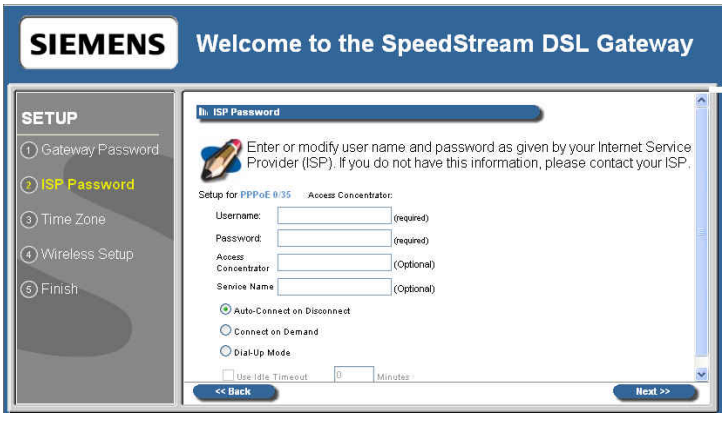
The first time you connect to the Gateway, the Setup Wizard runs automatically. (The Setup Wizard also runs if the Gateway's default settings are restored.) Proceed through the entire Setup Wizard to ensure accuracy of the installation.

You will need to know the username and password for Internet service provided by your ISP. Check the information supplied by your ISP for details.

1. The first window of the Setup Wizard is the "**Welcome"** window. Click **Next** on the "Welcome" window to begin setup. This displays the "Gateway Administrator Setup" window.

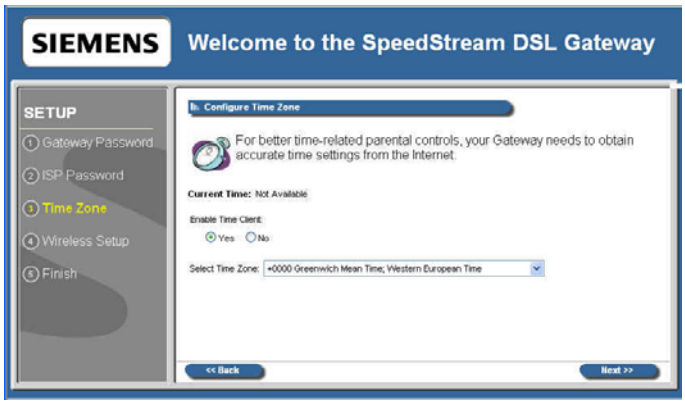

SIEMENS
Welcome to the SpeedStream DSL Gateway
SETUP
1 Gateway Password
2 ISP Password
3 Time Zone
4 Wireless Setup
5 Finish
Gateway Administrator Setup
Your Gateway requires someone to be the Gateway Administrator. This person has responsibility for adding user profiles, setting each person's access rights, and configuring the Gateway.
Please create a user name and password for the Gateway administrator.
REMEMBER THIS INFORMATION! This will be needed for future access and configuration of the Gateway.
User Name: admin (required)
New Password: (required)
Confirm Password: (required)
<< Back
Next >>

2. An administrator account has access rights to the Gateway configuration windows. Optionally, change the "admin" user name to a different administrative name by typing the new administrative name in **User Name**. If you wish, simply leave the "admin" user name in **User Name**.
3. Type a password in **New Password** and re-type it in **Confirm Password**.
4. Click **Next**. This displays the "ISP Password" window.



5. Enter information as specified by your ISP.

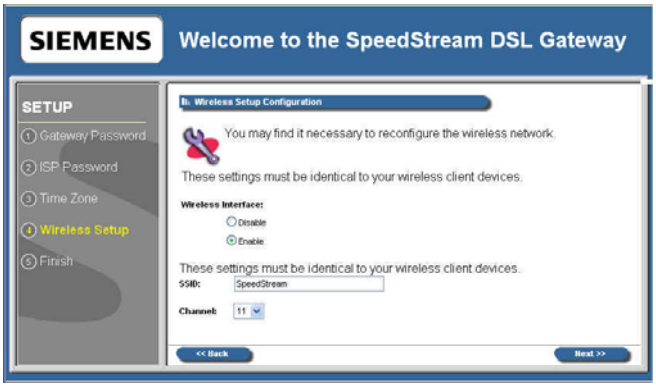
6. Click **Next**. This displays the "Configure Time Zone" window.



Optionally set the time zone of the area of the world in which you live on the "Configure Time Zone" window. This option must be enabled to define time of day restrictions for users.

7. To set the time zone, select the **Yes** option for **Enable Time Client**.

8. Select your time zone from the **Select Time Zone** drop-down menu, then click **Next**. This displays the "Wireless Setup Configuration" window.



Optionally set up wireless clients on your Gateway from the "Wireless Setup Configuration" window.

9. To setup wireless clients, select one of the following **Wireless Interface** options:

   - Select **Enable** to enable a wireless connection for your computer.
   - Select **Disable** if you do not wish to configure the Gateway for wireless, then click **Next**. This displays the "Finish" window.

10. If you selected **Enable**, enter your wireless network ID in **SSID** (Service Set Identifier). This value is the name of your network and must be identical to that defined for all the wireless client devices connected to your network.

11. Optionally select a channel from the **Channel** drop-down menu. The channel is a path of communication to use across your network. The selected channel must be identical to that defined for all the wireless client devices connected to your network. Depending on your area and Gateway configuration, the channel may default to only one value.

12. Click **Next**. This displays the "Wireless Security Configuration" window.

Set the wireless security level from the "Wireless Security Configuration" window. **ALL** wireless devices attached to the Gateway **MUST** have the same wireless security settings for your network to have proper communications and security.

13. From the **Security Mode** drop-down menu, select one of the following options:

- **Disable Security**
  Disables encryption, providing no wireless security for the Gateway.
- **WEP 64-bits**
  Wireless Equivalency Privacy. This option offers 64-bit encryption, which is the least secure WEP option. Please see the section in this document titled Wireless Setup WEP 64-Bit Option for more information.
- **WEP 128-bits**
  Wireless Equivalency Privacy. This option offers 128-bit encryption, which is a most secure WEP option. Please see the section in this document titled Wireless Setup WEP 128-Bit Option for more information.
- **WPA PSK**
  Wi-Fi Protected Access. WPA security changes encryption keys after a specified amount of time. This is the most secure option for wireless networks. Please see the section in this document titled Wireless Setup WPA PSK Option for more information.

14. Once you click **Next** on the final wireless setup window, one of the following happens:

- If you have a Powerline enabled Gateway, the "Powerline Filter Configuration" window is displayed.
- If you do not have a Powerline enabled Gateway, the "Finish" window is displayed.

15. If the Powerline window appears, select one of the following **Powerline Interface** options:

    - **Disable**
      Powerline connection is disabled. Click **Next**. This displays the "Finish" window.
    - **Enable**
      Powerline connection is enabled.

16. If you selected **Enable**, enter a password to secure your powerline connection. This password must be identical on all powerline client devices.
17. Select one the following from the **Security Level** drop-down menu.

    - **Off**
      Powerline encryption is turned off.
    - **On**
      Powerline encryption is turned on.

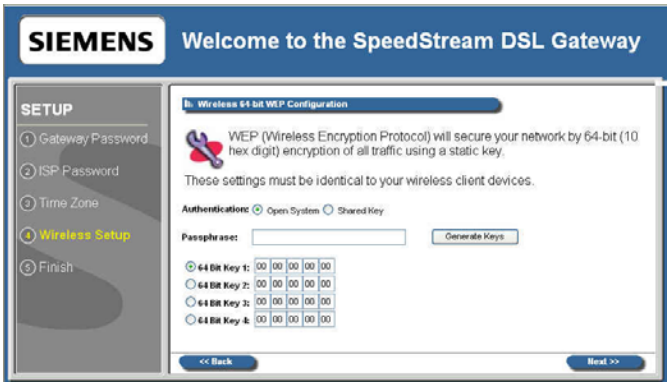
18. Click **Next**. This displays the "Finish" window.
19. On the "Finish" window, click **Finish**. This displays the "What do I do now?" window. From this window you may click one of the following:

    - **Surf Now**
      Your Web browser re-directs you to default home page of the Web browser you are using. You may return to the Gateway's configuration interface at anytime should you choose to further configure the Gateway.
    - **Continue**
      Displays the "Home" window where you can create usage profiles/rules for different users, change the level or type of security used on the Gateway, or define/configure your network to be managed by the Gateway.

Wireless Setup WEP 64-Bit Option

WEP security offers the same security offered by a wired LAN with encrypted packets. This option offers 64-bit encryption, which is the least secure WEP option. This section assumes you currently have the "Wireless Security Configuration" window displayed on your computer. To use the WEP 64-bit option:

1. Select the WEP 64-bits option from the **Security Mode** drop-down menu.
2. Click **Next**. This displays the "Wireless 64-bit WEP Configuration" window.

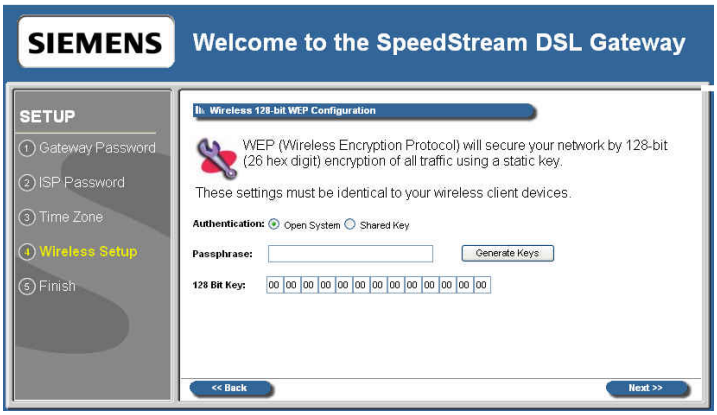

SIEMENS
Welcome to the SpeedStream DSL Gateway
SETUP
1 Gateway Password
2 ISP Password
3 Time Zone
4 Wireless Setup
5 Finish
Wireless 64 bit WEP Configuration
WEP (Wireless Encryption Protocol) will secure your network by 64-bit (10 hex digit) encryption of all traffic using a static key.
These settings must be identical to your wireless client devices.
Authentication: Open System Shared Key
Passphrase:
Generate Keys
64 Bit Key 1: 00 00 00 00 00
64 Bit Key 2: 00 00 00 00 00
64 Bit Key 3: 00 00 00 00 00
64 Bit Key 4: 00 00 00 00 00
<< Back
Next >>

3. Select one of the following **Authentication** options:
   - **Open System**
     Open system keys are always authenticated at the device level. After authentication, data is encrypted between the Gateway and the connected device. This is the weakest form of security and should not be used for sensitive data.
   - **Shared Key**
     Shared keys accepts a string of unencrypted data from a device. The Gateway encrypts with a WEP key and sends back the encrypted data to the attached device.
4. Type a phrase in **Passphrase**. The passphrase is used to generate the 64-bit keys. The passphrase can be between 1 and 32 characters.
5. Click **Generate Keys**. The system responds by generating keys that display in the boxes under **Passphrase**. Four different keys are generated.
6. Select one of the four keys to use for encryption.
7. Click **Next**. One of the following happens:
   - If you have a Powerline enabled Gateway, the "Powerline Filter Configuration" window is displayed.
   - If you do not have a Powerline enabled Gateway, the "Finish" window is displayed.

Wireless Setup WEP 128-Bit Option

WEP security offers the same security offered by a wired LAN with encrypted packets. This option offers 128-bit encryption, which is the most secure WEP option. This section assumes you currently have the "Wireless Security Configuration" window displayed on your computer. To use the WEP 128-bit option:

1. Select the WEP 128-bits option from the **Security Mode** drop-down menu.
2. Click **Next**. This displays the "Wireless 128-bit WEP Configuration" window.

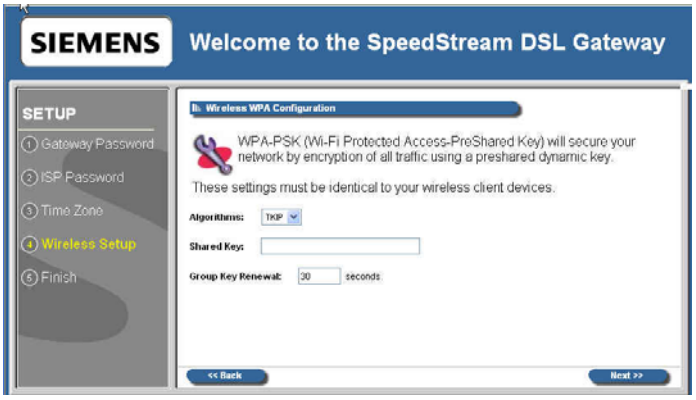

SIEMENS
Welcome to the SpeedStream DSL Gateway
SETUP
1 Gateway Password
2 ISP Password
3 Time Zone
4 Wireless Setup
5 Finish
Wireless 128-bit WEP Configuration
WEP (Wireless Encryption Protocol) will secure your network by 128-bit (26 hex digit) encryption of all traffic using a static key.
These settings must be identical to your wireless client devices.
Authentication: Open System Shared Key
Passphrase:
Generate Keys
128 Bit Key:
00 00 00 00 00 00 00 00 00 00 00 00 00
<< Back
Next >>

3. Select one of the following **Authentication** options:
   - **Open System**
     Open system keys are always authenticated at the device level. After authentication, data is encrypted between the Gateway and the connected device. This is the weakest form of security and should not be used for sensitive data.
   - **Shared Key**
     Shared keys accept a string of unencrypted data from a device. The Gateway encrypts with a WEP key and sends back the encrypted data to the attached device.
4. Type a phrase in **Passphrase**. The passphrase is used to generate the 124-bit key. The passphrase can be between 1 and 32 characters.
5. Click **Generate Keys**. The system responds by generating keys that display in the boxes under **Passphrase**.
6. Select one of the keys to use for encryption.
7. Click **Next**. One of the following happens:
   - If you have a Powerline enabled Gateway, the "Powerline Filter Configuration" window is displayed.
   - If you do not have a Powerline enabled Gateway, the "Finish" window is displayed.

Wireless Setup WPA PSK Option

WPA security changes encryption keys after a specified amount of time. This is the most secure option for wireless networks. This section assumes you currently have the "Wireless Security Configuration" window displayed on your computer. To use the WPA option:

1. Select the WPA-PSK option from the **Security Mode** drop-down menu.
2. Click **Next**. This displays the "Wireless WPA Configuration" window.


SIEMENS
Welcome to the SpeedStream DSL Gateway
SETUP
1 Gateway Password
2 ISP Password
3 Time Zone
4 Wireless Setup
5 Finish
Wireless WPA Configuration
WPA-PSK (Wi-Fi Protected Access-PreShared Key) will secure your network by encryption of all traffic using a preshared dynamic key.
These settings must be identical to your wireless client devices.
Algorithms: TKIP
Shared Key:
Group Key Renewal: 30 seconds
<< Back
Next >>

3. The "Wireless WPA Configuration" window is used to configure the algorithm, shared key, and key renewal options. Select one of the following options from the **Algorithms** drop-down menu:

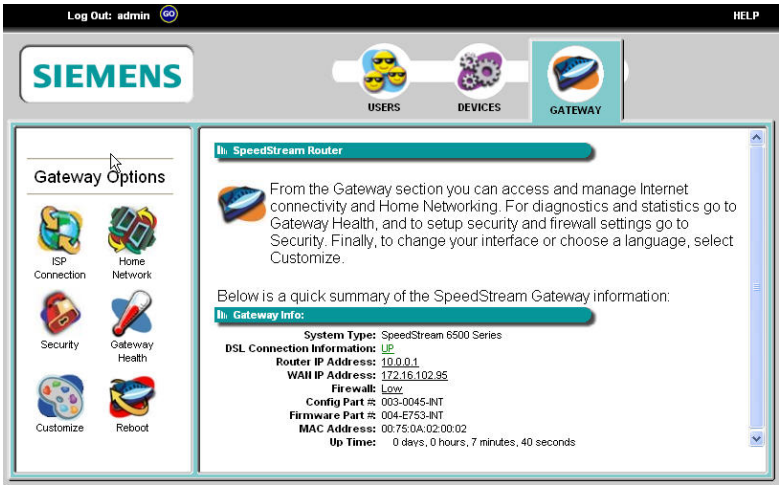
   - **TKIP**
     Temporal Key Integrity Protocol is a more powerful security protocol than WEP. This option verifies the security configuration after encryption keys are determined, synchronizes changing of the unicast encryption key for each frame, and determines a unique starting unicast encryption key for each pre-shared key authentication.
   - **AES**
     Advanced Encryption Standard supports a private key algorithm that ranges from 128 to 256 bits.

4. Type a key in **Shared Key**. The shared key is used to generate a dynamic encryption key for Gateway security.
5. Type a numeric value (in seconds) in **Group Key Renewal** to specify time to lapse between changing the key. The minimum time value is 30.
6. Click **Next**. One of the following happens:

   - If you have a Powerline enabled Gateway, the "Powerline Filter Configuration" window is displayed.
   - If you do not have a Powerline enabled Gateway, the "Finish" window is displayed.

Home Window

After finishing the Setup Wizard and clicking **Configure**, the Home window appears. This window also appears from now on when connecting to the Gateway.


Log Out: admin
HELP
SIEMENS
USERS
DEVICES
GATEWAY
Gateway Options
ISP Connection
Home Network
Security
Gateway Health
Customize
Reboot
SpeedStream Router
From the Gateway section you can access and manage Internet connectivity and Home Networking. For diagnostics and statistics go to Gateway Health, and to setup security and firewall settings go to Security. Finally, to change your interface or choose a language, select Customize.
Below is a quick summary of the SpeedStream Gateway information:
Gateway Info:
System Type: SpeedStream 6500 Series
DSL Connection Information: UP
Router IP Address: 10.0.0.1
WAN IP Address: 172.16.102.95
Firewall: Low
Config Part #: 003-0045-INT
Firmware Part #: 004-E753-INT
MAC Address: 00:75:0A:02:00:02
Up Time: 0 days, 0 hours, 7 minutes, 40 seconds

After finishing the Setup Wizard and clicking Configure, the "Home" window is displayed. This window is also displayed from now on when connecting to the Gateway. At the top of this window is the MenuBar that contains the login/logout drop-down menu and Help menu.

Below the Menu Bar is a Toolbar that contains a set of buttons to access various configuration and information windows on the Gateway: Users, Devices, Gateway. In the left navigation pane there are configuration options for the selected Toolbar button. These options differ depending on how a user is logged into the system. An administrator has full configuration rights (shown above), while a user has limited configuration rights. To Home window displays basic networking attributes of the modem including IP address and default gateway specifications.

Pay special attention to **Login** in the top left-hand corner of the window to ensure that you are logged in to access all available features.

Menu Bar

The only two items on the menu bar are the **Log in** drop-down menu and the **Help** menu option. The **Log In** drop-down menu is used to log in a user or administrator. The **Help** option is used to display a help system for the Gateway.

Toolbar

The Gateway has three primary toolbar buttons: Users, Devices, and Gateway. The options for all the toolbar buttons differ depending on the user login. The administrator has the most authority with all options enabled, while the user has limited options based on the user profile for the login. Please see the table below for more information.

	Users Button: This button provides access to user profiles and the User Profile Wizard. This wizard guides you through the steps required to set up and configure individual user profiles. Once configured, you can use this option to view a user's profile.
	Devices Button: This button provides Access to network devices connected to the Gateway. You can use this option to view shared files and resources on other computers if they are shared via Windows File Sharing.
	Gateway Button: This button provides access to all Gateway configuration options, security settings, Gateway health monitoring, and Internet connection and network details. The settings available may differ depending upon your service provider.

Logging into the Gateway

There are two types of primary users that log into the Gateway: administrators and users. Administrators have rights to all of the configuration options available on the Gateway. Users have limited access based on what is set by the administrator for each user.

To log on to the Gateway:

1. Select a user from the **Log In** drop-down menu in the upper-left corner of the "Home" window.
2. Select a user from the **Username** drop-down menu.
3. Type the user password in **Password**.
4. Click **Go**. This displays the "Home" window.

Logging out of the Gateway

To log out of the Gateway:

1. Click **GO** next to **Log Out**. The system responds by displaying the "Home" window.

Chapter 5

Configuring Users and Devices

This chapter explains how to configure users and devices on the Gateway.

This chapter contains details for configuring users and devices on the Gateway. This chapter is organized into two parts corresponding to the buttons in the toolbar: Users and Devices. Refer to Chapter 6, Configuring Gateway Options for details on configuring the features on the Gateway.

Configuring Users

Users are added and maintained from the "User Profiles" window accessed by clicking **Users** button on the toolbar. The "User Profiles" window provides details about all active user profiles if **Enable User Profiling** is selected.

SIEMENS
USERS
DEVICES
GATEWAY
User Profiles
From here you can create and manage a User Profile for each person in your home or office and set parental controls. By enabling user profiling, you can monitor when and where each person goes on the Internet. To add a new user, click the 'Add New User' icon.
To activate these features, check the box below. When User Profiling is turned on, each new user will be forced to log in before surfing the web.
Enable User Profiling
Users Summary
Profile
Logged into
Last Viewed
admin
PM902867 - 10.0.0.2
eni
Delete
Monitor
Users
eni
Add New User

The **Enable User Profiling** option must be selected on the "User Profiles" window for the content filtering option to be operational.

Adding a User

This section describes how to add users to the Gateway to restrict their access to Gateway functions and to the Internet. You **MUST** be logged in as the administrator to add a user.

To add a user:

1. From the "Users Profile" window, click the **Add New User** button in the left navigation pane. This displays the "Profile User Information" window.

2. Type a user name in **Username**.
3. Type a password in **Password**.
4. Re-type the password in **Confirm**.
5. Click **Next**. This displays the "Profile Content Filtering" window. (At any time during user configuration, you can click **Finish** to complete the user profile and accept the defaults for this user.)

SIEMENS
USERS
DEVICES
GATEWAY
User Setup:
1 Enter Username
2 Content Filtering
3 Security Level
4 Time Settings
5 Computer
6 Customize
7 Finished
Profile Content Filtering
Content Filtering lets you control what Internet sites this user can visit.
Select the type of Content Filtering for this user:
Disable all Content Filtering - This user can surf to any site, and no site access will be logged for monitoring purposes.
Allow access only to website addresses containing the following words:
Deny all access to website addresses containing the following words:
Website word/name
Edit
Delete
Table is Empty
Add Entry
Learn More
<< Back
Cancel
Next >>
Finish

Content filtering restricts access to undesirable Web sites and Web content. The **Enable User Profiling** option must be selected on the "User Profiles" window for the content filtering option to be operational.

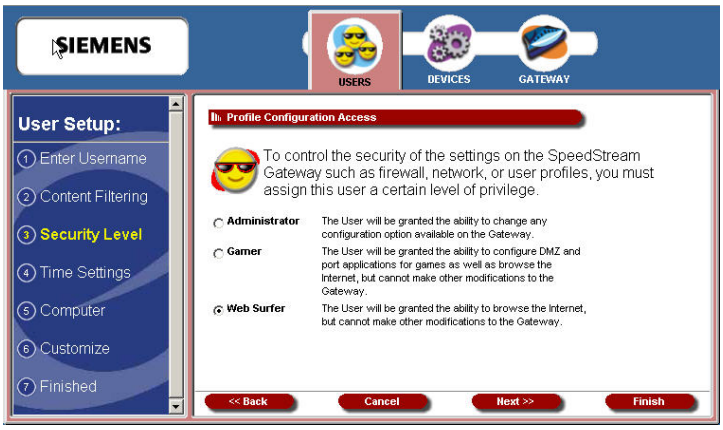
6. Select one of the following content filtering options:

   - **Disable all Content Filtering**
     User has access to all Internet content without restrictions.
   - **Allow access only to website addresses containing the following words**
     User has access only to the specified Web addresses or to addresses containing specified word entries defined in the Website word/name table.
   - **Deny all access to website addresses containing the following words**
     User is denied access to all Web addresses specified as well as addresses that contain any words specified in the Website word/name table.

7. If the **Allow access only…** or **Deny all access…** option is selected, type a word or Web address in the box under the Website word/name table, then click **Add Entry**. The system responds by adding the word or Web address to the Website word/name table.

   Note: The entries in the Website word/name table may be either modified or deleted at any time by clicking either **Edit** or **Delete** next to the corresponding word or Web address.

8. Click **Next**. This displays the "Profile Configuration Access" window.

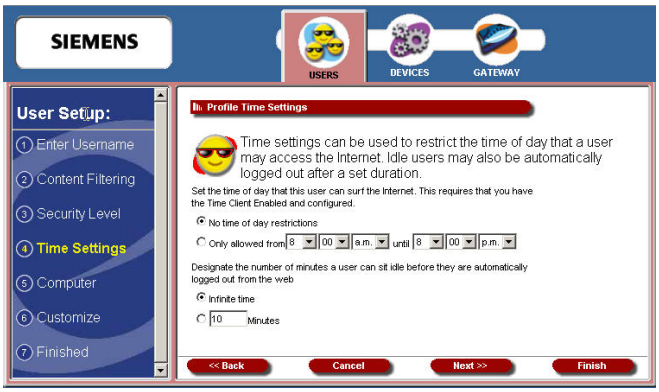

SIEMENS
USERS
DEVICES
GATEWAY
User Setup:
1 Enter Username
2 Content Filtering
3 Security Level
4 Time Settings
5 Computer
6 Customize
7 Finished
Profile Configuration Access
To control the security of the settings on the SpeedStream Gateway such as firewall, network, or user profiles, you must assign this user a certain level of privilege.
Administrator The User will be granted the ability to change any configuration option available on the Gateway.
Gamer The User will be granted the ability to configure DMZ and port applications for games as well as browse the Internet, but cannot make other modifications to the Gateway.
Web Surfer The User will be granted the ability to browse the Internet, but cannot make other modifications to the Gateway.
<< Back
Cancel
Next >>
Finish

Profile configuration access defines the access permission for a user controlling what functions and features are available to that user.

9. Select one of the following profiles and click.

   - **Administrator**
     User has access to the Internet and all of the configuration tools on the Gateway.
   - **Gamer**
     User has access to the Internet as well as the Gateway's commonly used tools for gamers, including Port Configuration and DMZ.
   - **Web Surfer**
     Use has access only to the Internet, not to the Gateway's configuration.

10. Click **Next**. This displays the "Profile Time Setting" window.


SIEMENS
USERS
DEVICES
GATEWAY
User Setup:
1 Enter Username
2 Content Filtering
3 Security Level
4 Time Settings
5 Computer
6 Customize
7 Finished
Profile Time Settings
Time settings can be used to restrict the time of day that a user may access the Internet. Idle users may also be automatically logged out after a set duration.
Set the time of day that this user can surf the Internet. This requires that you have the Time Client Enabled and configured.
No time of day restrictions
Only allowed from 8 00 a.m. until 8 00 p.m.
Designate the number of minutes a user can sit idle before they are automatically logged out from the web
Infinite time
10 Minutes
<< Back
Cancel
Next >>
Finish

Profile time settings are used to limit a user's ability to use the Internet during certain times of the day or night. You can also define the amount of time a user stays logged on to the Internet without Web surfing activity (Idle Time). To use the time of day restrictions, you must have the Time Client enabled. Please see the Setup Wizard section for more information.

11. Select one of the following time of day options to control the time of day a user can access the internet:

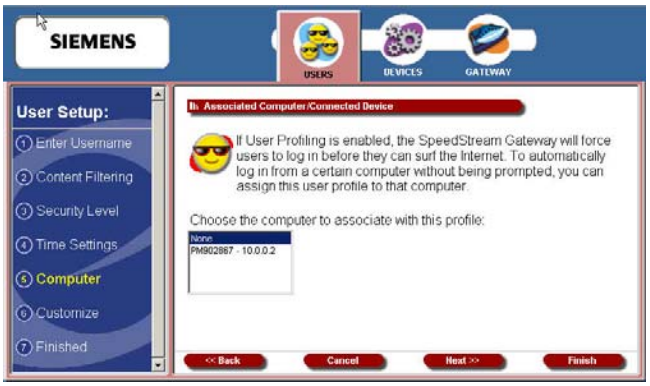
   - **No time of day restrictions**
     The user can access the Internet at any time.

- **Only allowed from**
  The user can only access the Internet at the time range set in the time drop-down menus. Be sure to specify the **from** and **until** times the user can access the Internet.

12. Select one of the following options to designate the number of minutes a user can sit idle before they are automatically logged out from the web:

    - **Infinite Time**
      The user is never automatically logged out of the Internet.
    - **Minutes**
      Type a time interval in minutes in **Minutes**. This time represents how long a user may be idle before automatically being logged out of the Internet.

13. Click **Next**. This displays the "Associated Computer/Connected Device" window.


SIEMENS
USERS
DEVICES
GATEWAY
User Setup:
1 Enter Username
2 Content Filtering
3 Security Level
4 Time Settings
5 Computer
6 Customize
7 Finished
Associated Computer/Connected Device
If User Profiling is enabled, the SpeedStream Gateway will force users to log in before they can surf the Internet. To automatically log in from a certain computer without being prompted, you can assign this user profile to that computer.
Choose the computer to associate with this profile:
None
PM902887 - 10.0.0.2
<< Back
Cancel
Next >>
Finish

Some users consistently use a particular computer to surf the Internet. To simplify logging in for these users, you can use the Associated Computer option to automatically log a particular user into the Gateway with their username and password when they access the Internet from the specified computer.

14. Select one of the following:

    - A specific device to associate with the profile. All computers and devices currently on the network, powered on, and detected by the Gateway are displayed in the computer list.
    - **None.** The user can log in from any device.

15. Click **Next**. This displays the "Customized Profile Icon" window.

All user profiles have an icon that displays in the left navigation pane of the "User Profiles" window. You may customize the color of this icon using the "Customized Profile Icon" window.

16. To select a color, do one of the following:

- Select a color from the drop-down menu.
- Type a numeric color value in the box next to the color drop-down menu. The number is based on RGB (Red Green Blue) values. For example, the color red is represented by a value of ff0000, green is represented by a value of 00ff00, and blue is represented by a value of 0000ff. **Note**: If you are entering a numeric value for the color, ensure that the "#" is in front of your numeric value.

17. Click **Finish**. This displays the "User Profile" window. The icon of the user you just created is displayed in the left navigation pane.

Editing A User Profile

This section describes how to edit a user profile. You must be logged in as the administrator to edit a user profile.

To edit a user profile:

1. From the "Users Profile" window, click the button in the left navigation pane corresponding to the user you want to edit. This displays the "Profile Monitor" window.

2. Click **Edit Profile**. This displays the "Profile Content Filtering" window with the **User Setup** pane in the left navigation pane.

SIEMENS
USERS
DEVICES
GATEWAY
User Setup:
1 Enter Username
2 Content Filtering
3 Security Level
4 Time Settings
5 Computer
6 Customize
7 Finished
Profile Content Filtering
Content Filtering lets you control what Internet sites this user can visit.
Select the type of Content Filtering for this user:
Disable all Content Filtering - This user can surf to any site, and no site access will be logged for monitoring purposes.
Allow access only to website addresses containing the following words:
Deny all access to website addresses containing the following words:
Website word/name
Edit
Delete
Table is Empty
Add Entry
Learn More
<< Back
Cancel
Next >>
Finish

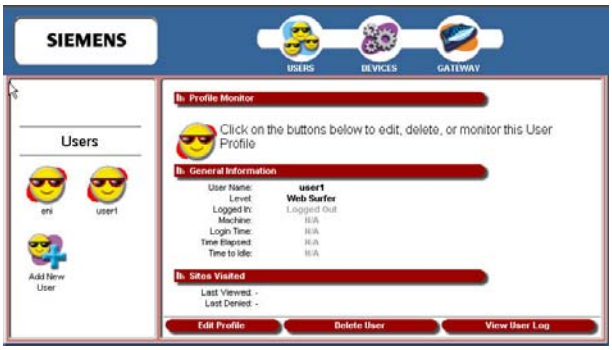
3. Click on any item in the **User Setup** list to display the appropriate window.
4. Make any changes.
5. Once you have made all the changes you want, click **Finish**.

Deleting a User

This section describes how to delete a user. You must be logged in as the administrator to delete a user.

To delete a user:

1. From the "Users Profile" window, click the button in the left navigation pane corresponding to the user you want to delete. This displays the "Profile Monitor" window.



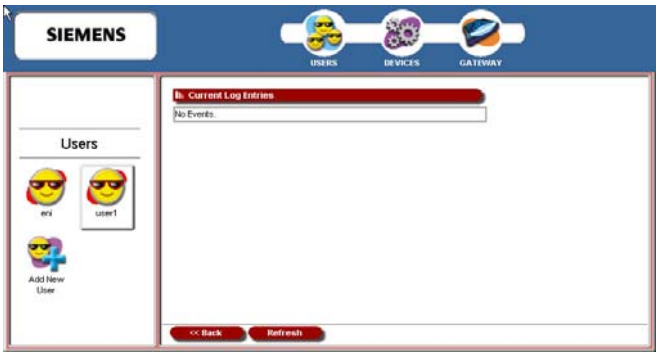
2. Click **Delete User**.

Viewing User Logs

User logs provide time stamped information about the activity of the user over the network.

To view user logs:

1. From the "Users Profile" window, click the button in the left navigation pane corresponding to the user you want to delete. This displays the "Profile Monitor" window.
2. Click **View User Log**. This displays the "Current Log Entries" window displaying all the log information about the user.

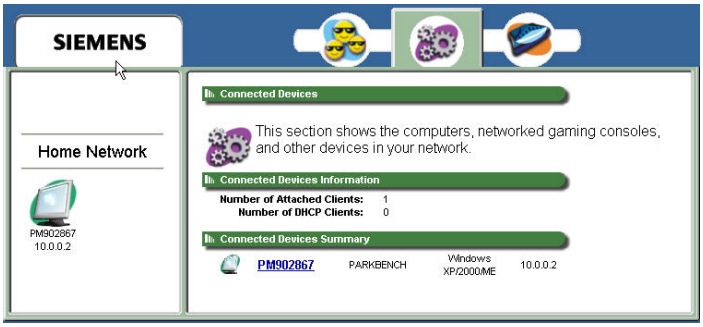


Configuring Devices

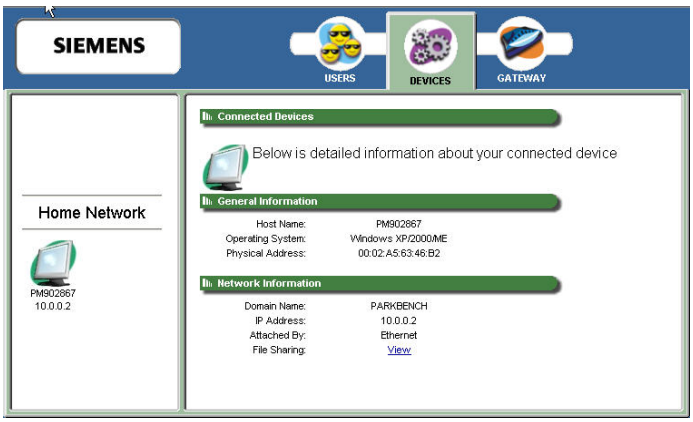
The Devices option allows you to view devices connected to your Gateway. If you are logged in as the administrator, you can view all the connected devices to the Gateway. If you are logged in as a specific user, you can only view devices associated with that user logon.

To use the Devices option:

1. Click **Devices** in the toolbar. This displays the "Connected Devices" window displaying general information about devices on your network.



2. Click the icon of a connected device in the left navigation pane, or click the device hyperlink under **Connected Devices Summary**. This displays the "Connected Devices" window, which displays both general and network information about the selected device.



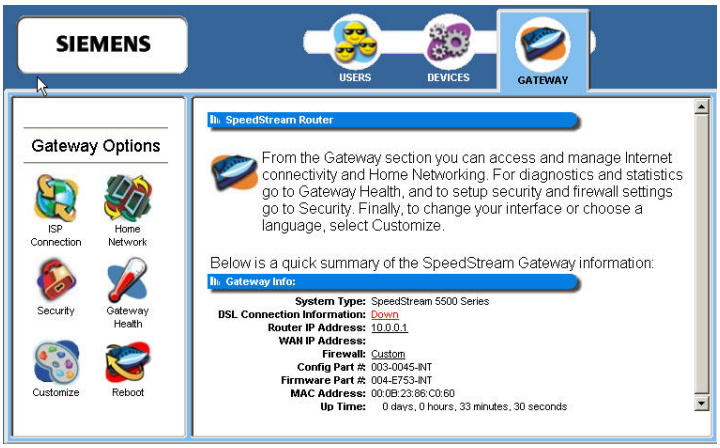
Chapter 6

Configuring Advanced Features

This chapter explains how to configure advanced features on the Gateway.

This chapter contains details for configuring the many advanced features available with your Gateway. Some of the features described below require at least a mid-level understanding of networking principles. These features are provided to allow configuration flexibility for advanced users.

These advanced features are accessed through the **Gateway** button available on the toolbar on the "Main" window. The options that display under the **Gateway Options** pane in the left navigation pane are based on how you logged into the system. If you logged in as the administrator, all options are turned on and enabled. If you logged in as a user, only the Gateway Health, Customize, and Reboot options are enabled.


SIEMENS
USERS
DEVICES
GATEWAY
Gateway Options
ISP Connection
Home Network
Security
Gateway Health
Customize
Reboot
SpeedStream Router
From the Gateway section you can access and manage Internet connectivity and Home Networking. For diagnostics and statistics go to Gateway Health, and to setup security and firewall settings go to Security. Finally, to change your interface or choose a language, select Customize.
Below is a quick summary of the SpeedStream Gateway information:
Gateway Info:
System Type: SpeedStream 5500 Series
DSL Connection Information: Down
Router IP Address: 10.0.0.1
WAN IP Address:
Firewall: Custom
Config Part #: 003-0045-INT
Firmware Part #: 004-E753-INT
MAC Address: 00:0B:23:86:C0:60
Up Time: 0 days, 0 hours, 33 minutes, 30 seconds

Gateway Options discussed in this chapter

This chapter is organized into parts that correspond to the following buttons shown in the **Gateway Options** pane.

Get information about ISP connections. You can also use this option to set ISP configuration parameters. This should only be done when instructed by your ISP.

View network-related information

Configure security for the Gateway.

Reboot the Gateway.

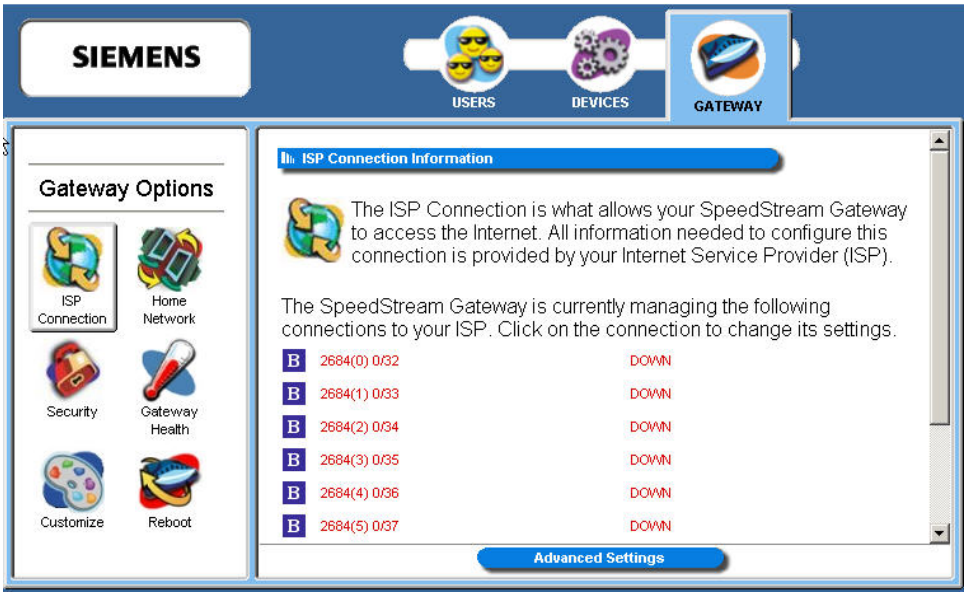
ISP Connection

The **ISP Connection** option displays all active and available Internet connections. Many of the settings for this option are intended for use only by advanced users. This option may not be available depending on your ISP. You must be logged in as an administrator to use this option.

WARNING: If this feature is not properly configured your Internet connection may terminate.

To use the ISP connection function:

1. Click the **ISP Connection** button in the left navigation pane. This displays the "ISP Connection Information" window listing all the ISP connections being managed by the Gateway.

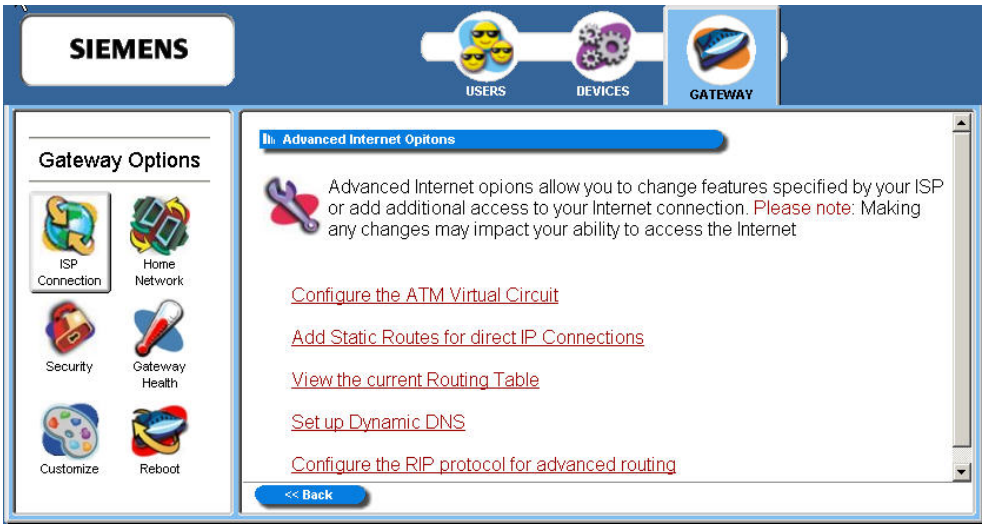

SIEMENS
USERS
DEVICES
GATEWAY
Gateway Options
ISP Connection
Home Network
Security
Gateway Health
Customize
Reboot
ISP Connection Information
The ISP Connection is what allows your SpeedStream Gateway to access the Internet. All information needed to configure this connection is provided by your Internet Service Provider (ISP).
The SpeedStream Gateway is currently managing the following connections to your ISP. Click on the connection to change its settings.
2684(0) 0/32 DOWN
2684(1) 0/33 DOWN
2684(2) 0/34 DOWN
2684(3) 0/35 DOWN
2684(4) 0/36 DOWN
2684(5) 0/37 DOWN
Advanced Settings

2. Click one of the ISP connections (in red) to reconfigure that connection. Please check with your ISP for the information required to reconfigure a connection.
3. Optionally refer to the section titled Advanced Settings for details on configuring advanced ISP connection settings.

Advanced ISP Settings

The Gateway provides access to additional, advanced ISP configuration settings. All the options in this section should only be configured with the help and guidance of your ISP. Incorrect changes to any of these options could result in the failure of your Internet connection.

To access the advanced settings, click **Advanced Settings** from the "ISP Connection Information" window. This displays the "Advanced Internet Options" window.


SIEMENS
USERS
DEVICES
GATEWAY
Gateway Options
ISP Connection
Home Network
Security
Gateway Health
Customize
Reboot
Advanced Internet Opitons
Advanced Internet opions allow you to change features specified by your ISP or add additional access to your Internet connection. Please note: Making any changes may impact your ability to access the Internet
Configure the ATM Virtual Circuit
Add Static Routes for direct IP Connections
View the current Routing Table
Set up Dynamic DNS
Configure the RIP protocol for advanced routing
<< Back

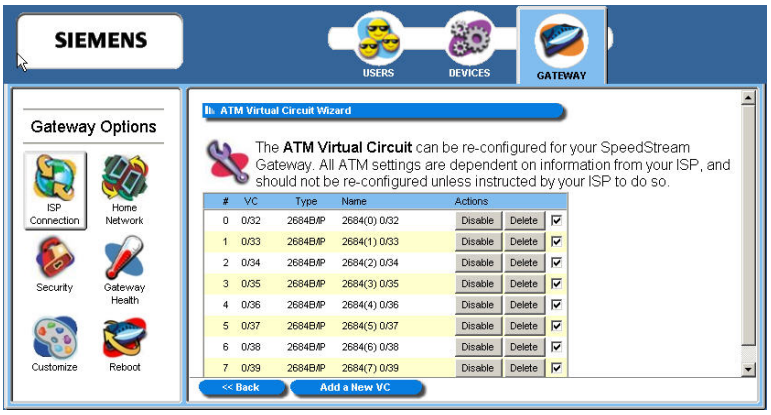
The advanced options are listed below. To access one of these options, click its link on the "Advanced Internet Options" window.

Configure the ATM Virtual Circuit	Create and configure a PVC (Permanent Virtual Circuit) across a network. A PVC is used to maintain a permanent connection between two points on a network.
Add Static Routes for direct ISP Connections	Configure static routes to remote equipment. Static routing allows a pre-defined route to be set for the transmission of data.
View the Current Routing Table	View a table of routing information of all static and dynamic routes for network devices.
Set up Dynamic DNS	Set up dynamic DNS. Dynamic DNS translates IP addresses into alphanumeric names.
Configure the RIP protocol for advanced routing	Configure the protocol that allows the Gateway to determine the shortest path between two points on the network.

ATM Virtual Circuits

Use the ATM virtual circuit advanced option to create and configure a Permanent Virtual Circuit (PVC). A PVC is used to maintain a permanent connection between two points on a network. Changes to ATM settings should not be made unless you are advised to do so by your Internet Service Provider.

To access the ATM virtual circuit option, click the **Configure ATM Virtual Circuit** hyperlink on the "Advanced Internet Options" window. This displays the "ATM Virtual Circuit Wizard" window.


SIEMENS
USERS
DEVICES
GATEWAY
Gateway Options
ISP Connection
Home Network
Security
Gateway Health
Customize
Reboot
ATM Virtual Circuit Wizard
The ATM Virtual Circuit can be re-configured for your SpeedStream Gateway. All ATM settings are dependent on information from your ISP, and should not be re-configured unless instructed by your ISP to do so.
VC Type Name Actions
0 0/32 2684B/P 2684(0) 0/32 Disable Delete
1 0/33 2684B/P 2684(1) 0/33 Disable Delete
2 0/34 2684B/P 2684(2) 0/34 Disable Delete
3 0/35 2684B/P 2684(3) 0/35 Disable Delete
4 0/36 2684B/P 2684(4) 0/36 Disable Delete
5 0/37 2684B/P 2684(5) 0/37 Disable Delete
6 0/38 2684B/P 2684(6) 0/38 Disable Delete
7 0/39 2684B/P 2684(7) 0/39 Disable Delete
<< Back
Add a New VC

Make any modifications advised by your ISP.

Static Routes

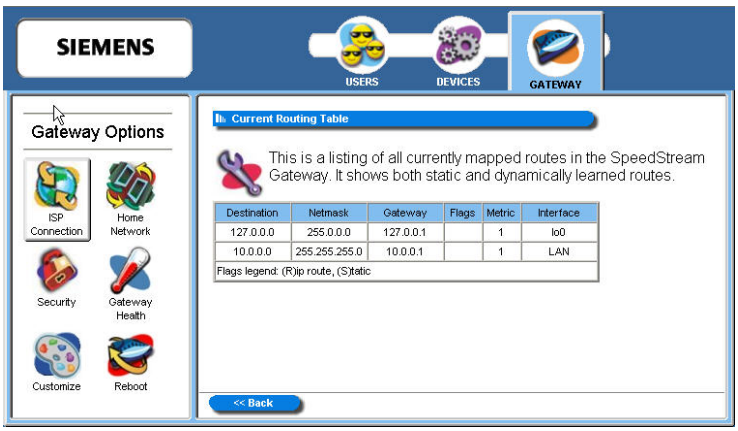
Use the static routes advanced option to configure static routes to remote equipment. Static routing allows a pre-defined route to be set for the transmission of data. Static routes take precedence over all dynamic routing options and also provide enhanced security over dynamic routing.

To configure the static routes:

1. Click the **Add Static Routes for Direct IP Connections** hyperlink from the "Advanced Internet Options" window. This displays the "Static Routes" window.

2. Type the IP address of the destination device in **Destination**.
3. Type the net mask of the destination device in **Net Mask**.
4. Optionally, type the IP address of a destination Gateway in **Next Hop**.
5. Select a connection type from the **Interface** drop-down menu.
6. Click **Apply**. The system responds by adding your new route to the routing table.

To view the current routing table, click the **View the current routing table** hyperlink. This displays a table of routing information including destination IP address, subnet mask, flags, Gateway, metric and interface of all static and dynamic routes for network devices.



Dynamic DNS

Use the dynamic DNS advanced option to set up dynamic DNS. Dynamic DNS translates IP addresses into alphanumeric names. For example, an IP address of 333.136.249.80 could be translated into siemens.com. To use the DDNS service, you must register for the service. You can register from the following web page: www.dydns.org/services/dydns.

Once registered, you must set up your DNS data on the Gateway. Once this is done users can connect to your servers (or DMZ computer) from the Internet using your Domain name. Refer to the section in this document titled DMZ for more information on DMZs.

To set up Dynamic DNS on the Gateway:

1. Click the **Set up Dynamic DNS** hyperlink from the "Advanced Internet Options" window. This displays the "Set Up Dynamic DNS" window.

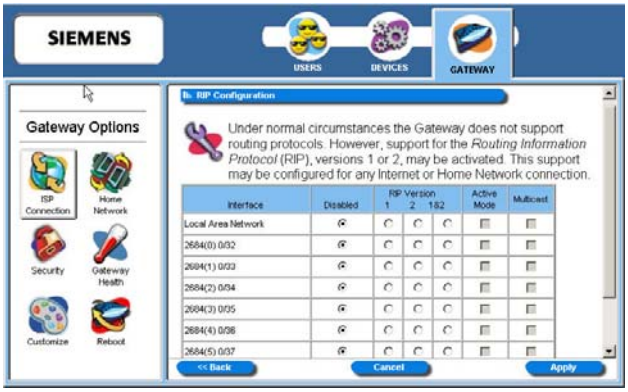
2. Select the **Enable** option.
3. Type the name provided to you by www.dydns.org in **Service Username**.
4. Type your www.dydns.org password in **Password**.
5. Type the domain or host name provided by www.dydns.org in **Host Name 1**.
6. Optionally, if you have more than one domain or host name, type it in **Host Name 2**.
7. Click **Apply**. The system responds by registering your domain or host name to www.dydns.org.

RIP (Routing Information Protocol)

Using RIP, the Gateway is able to determine the shortest distance between two points on the network based on the addresses of the originating devices. RIP (Routing Information Protocol) is based on distance algorithms to calculate the shortest path. The shortest path is based on the number of hops between two points.

To use the RIP option:

1. Click the **Configure the RIP protocol for advanced routing** hyperlink from the "Advanced Internet Options" window. This displays the "RIP Configuration" window.

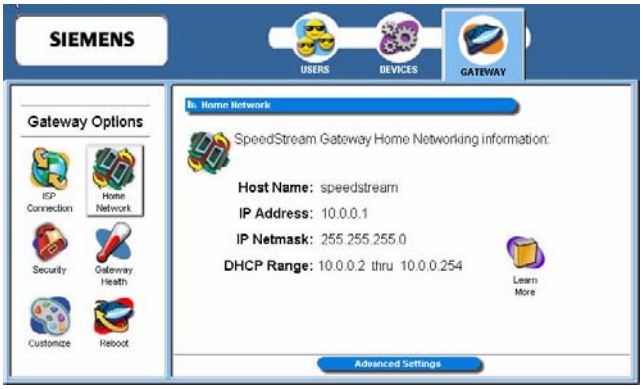


2. Select one of the following options from under the **RIP Version** heading next to the connection of your choice:
   - **1:** Provides essential RIP packet formatting for routing information packets.
   - **2:** Provides enhanced packet formatting for routing information packets by providing the following: IP address, subnet mask, next hop, and metric (shows how many routers the routing packet crossed to its destination.
   - **1&2:** A combination of both types of RIP packets.
3. Select an **Active Mode** checkbox next to a corresponding connection to enable it.
4. Click **Apply**. This displays the "Your Settings Have Been Saved" window.
5. Optionally, click **Reboot** if you wish for the settings to immediately be implemented. The system responds by restarting your Gateway.

Home Network

The Home Network option displays all network-related information. You must be logged in as the administrator to access this option. To use the Home Network option:

1. Click the **Home Network** button on the **Gateway Options** pane. This displays the "Home Network" window containing information about the home network.



2. Optionally, click **Advanced Settings** to display a list of advanced features that allow you to manage the computers on your network. This displays the "Advanced Home Networking" window.

SIEMENS
USERS
DEVICES
GATEWAY
Gateway Options
ISP Connection
Home Network
Security
Gateway Health
Customize
Reboot
Advanced Home Networking
Advanced features allow you to manage computers on your network. Please note: Making any changes may impact your ability to access the Internet.
Configure the Local SpeedStream Gateway IP Network
Configure the Local SpeedStream Gateway Server Ports
Configure the Local SpeedStream Gateway LAN/WAN Port
Configure the Local SpeedStream Gateway Wireless Network
Configure the Local SpeedStream Gateway Powerline Network
<< Back

The advanced options are listed below. To access one of these options, click its link on the "Advanced Home Networking" window.

IP Network	Define the range for assigning IP addresses.
Server Ports	Specify the ports used by common applications such as HTTP, FTP, and Telnet.
LAN/WAN Port	Configure Ethernet port #4 as either a LAN (network) port or as a WAN (Internet connection) port.
Wireless Network	Configure the wireless equipment in your Gateway.
Powerline Network	Configure security for the powerline network. This option is available only if your Gateway is configured for Powerline.
UPnP	Configure UPnP. UPnP allows the Gateway to communicate directly with certain Windows operating systems.

IP Network

The Gateway provides the flexibility to use different ranges of IP addresses to be assigned by the DHCP Server housed in the Gateway. DHCP (Dynamic Host Configuration Protocol) allows computers to obtain either permanent or temporary IP addresses from a central server.

To configure the IP network option:

1. Click the **Configure the local SpeedStream Gateway IP Network** hyperlink. This displays the "SpeedStream Gateway IP Network" window.

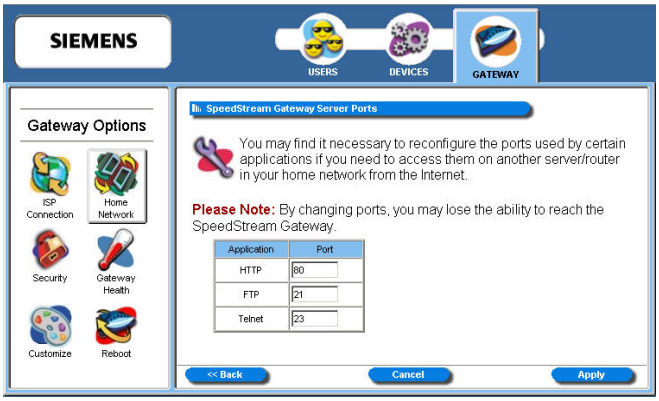
2. Select a range from the displayed options and click **Save Settings**. Be sure to select an IP address range that is not in conflict with any existing devices.
3. Optionally, click the **Custom Settings** hyperlink for advanced configuration. Please contact your ISP for more information on configuring the options for custom settings.

Server Ports

Common applications such as HTTP (Web site traffic), FTP, and Telnet use pre-defined incoming port numbers for compatibility with other services. If you wish to change the ports used by these applications you may do so using this option. This feature is recommended for use by advanced users only.

To configure the server port option:

1. Click the **Configure the Local SpeedStream Gateway Server Ports** hyperlink. This displays the "SpeedStream Gateway Server Ports" window.



2. Optionally, type a port number in **HTTP**. The default port for this field is 80.
3. Optionally, type a port number in **FTP**. The default port for this field is 21.
4. Optionally, type a port number in **Telnet**. The default port for this field is 23.
5. Click **Apply**. This displays the "Your settings have been saved" window.
6. Optionally, click **Reboot** if you wish for the settings to immediately be implemented. The system responds by restarting your Gateway.

LAN/WAN Port

If your Gateway contains four Ethernet ports, Ethernet port #4 can be used as either a LAN (network) port or as a WAN (Internet connection) port. Select the appropriate option to define whether the port is used as a fourth local network port or as a connection for another broadband device.

Note: For configuration of the port as a WAN port, you may be required to consult your Internet Service Provider for the appropriate settings.

To configure the LAN/WAN port:

1. Click the **Configure the Local SpeedStream Gateway LAN/WAN Port** hyperlink. This displays the "SpeedStream Gateway LAN/WAN Port" window.

2. Select one of the following options:

   - **LAN** (Local Area Network)
     Use the port as a connection to the network located in your home or premises.
   - **WAN** (Wide Area Network)
     Use the port as a connection to a large connected network such as the Internet that is spread over a large geographic area. If you select the WAN option, please contact your ISP for instructions on how to configure this option.

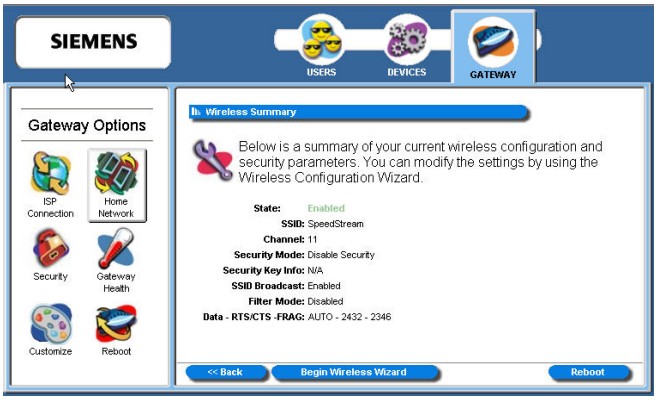
3. Click **Apply**.

Wireless Network

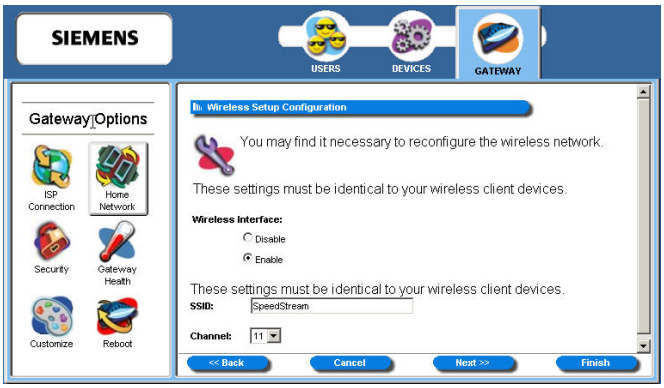
Configure the wireless network using this option. The wireless settings on the Gateway must match those of any wireless clients on your network.

To configure the wireless network:

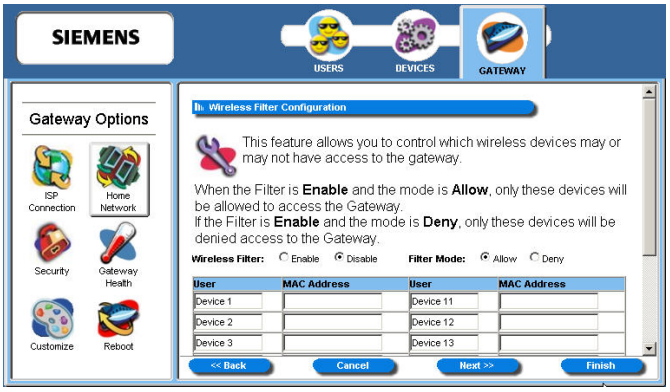
1. Click the **Configure the Local SpeedStream Gateway Wireless Network** hyperlink. This displays the "Wireless Summary" window.



2. Click **Begin Wireless Wizard**. This displays the "Wireless Setup Configuration" window.



3. Select **Enable** to enable the **Wireless Interface**.
4. Type your wireless network ID in **SSID** (Service Set Identifier).
5. Optionally, select a channel ID from the **Channel** drop-down menu. This is typically done if you experience any interference with your wireless Gateway.
6. Click **Next**. This displays the "Wireless Security Configuration" window.



Set the wireless security level from the "Wireless Security Configuration" window. All wireless devices attached to the Gateway **MUST** have the same wireless security settings for your network to have proper communications and security.

7. From the **Security Mode** drop-down menu, select one of the following options:

   - **WEP 64-bits**
     Wireless Equivalency Privacy. WEP security offers the same security offered by a wired LAN with encrypted packets. This option offers 64-bit encryption, which is the least secure WEP option. Please see the section in this document titled Wireless Setup WEP 64-Bit Option (Advanced Home Networking) for more information.

   - **WEP 128-bits**
     Wireless Equivalency Privacy. WEP security offers the same security offered by a wired LAN with encrypted packets. This option offers 128-bit encryption, which is a most secure WEP option. Please see the section in this document titled Wireless Setup WEP 128-Bit Option (Advanced Home Networking) for more information.

   - **WPA PSK**
     Wi-Fi Protected Access. WPA security changes encryption keys after a specified amount of time. This is the most secure option for wireless networks. Please see the section in this document titled Wireless Setup WPA PSK Option (Advanced Home Networking) for more information.

8. Optionally, select the **Enable SSID Broadcast** option so wireless users can see the existence of the wireless Gateway with the associated SSID.

Wireless Setup WEP 64-Bit Option (Advanced Home Network)

WEP security offers the same security offered by a wired LAN with encrypted packets. This section assumes you currently have the "Wireless Security Configuration" window displayed on your computer.

To use the WEP 64-bit option:

1. From the "Wireless Security Configuration" window, select **WEP 64-bits** from the **Security Mode** drop-down menu.
2. Click **Next**. This displays the "Wireless 64-bit WEP Configuration" window.

SIEMENS
USERS
DEVICES
GATEWAY
Gateway Options
ISP Connection
Home Network
Security
Gateway Health
Customize
Reboot
Wireless 64-bit WEP Configuration
WEP (Wireless Encryption Protocol) will secure your network by 64-bit (10 hex digit) encryption of all traffic using a static key.
These settings must be identical to your wireless client devices.
Authentication: Open System Shared Key
Passphrase:
Generate Keys
64 Bit Key 1: 00 00 00 00 00
64 Bit Key 2: 00 00 00 00 00
64 Bit Key 3: 00 00 00 00 00
64 Bit Key 4: 00 00 00 00 00
<< Back
Cancel
Next >>
Finish

3. Select one of the following **Authentication** options:
   - **Open System**
     Open system keys are always authenticated at the device level. After authentication, data is encrypted between the Gateway and the connected device. This is the weakest form of security and should not be used for sensitive data.
   - **Shared Key**
     Shared keys accept a string of unencrypted data from a device. The Gateway encrypts with a WEP key and sends back the encrypted data to the attached device.
4. Type a phrase in **Passphrase**. The passphrase is used to generate the 64-bit keys. The passphrase can be between 1 and 32 characters.
5. Click **Generate Keys**. The system responds by generating keys that display in the boxes under **Passphrase**. Four different keys are generated.
6. Select one of the four keys to use for encryption.
7. Click **Next**. This displays the "Wireless Filter Configuration" window.

Wireless Setup WEP 128-Bit Option (Advanced Home Network)

WEP security offers the same security offered by a wired LAN with encrypted packets. This option offers 128-bit encryption, which is the most secure WEP option. This section assumes you currently have the "Wireless Security Configuration" window displayed on your computer.

To use the WEP 128-bit option:

1. From the "Wireless Security Configuration" window, select **WEP 128-bits** from the **Security Mode** drop-down menu.
2. Click **Next**. This displays the "Wireless 128-bit WEP Configuration" window.

3. Select one of the following **Authentication** options:
   - **Open System**
     Open system keys are always authenticated at the device level. After authentication, data is encrypted between the Gateway and the connected device. This is the weakest form of security and should not be used for sensitive data.
   - **Shared Key**
     Shared keys accept a string of unencrypted data from a device. The Gateway encrypts with a WEP key and sends back the encrypted data to the attached device.
4. Type a phrase in **Passphrase**. The passphrase is used to generate the 128-bit key. The passphrase can be between 1 and 32 characters.
5. Click **Generate Keys**. The system responds by generating keys that display in the boxes under **Passphrase**.
6. Select one of the keys to use for encryption.
7. Click **Next**. This displays the "Wireless Filter Configuration" window.

Wireless Setup WPA PSK Option (Advanced Home Network)

WPA security changes encryption keys after a specified amount of time. This is the most secure option for wireless networks. This section assumes you currently have the "Wireless Security Configuration" window displayed on your computer.

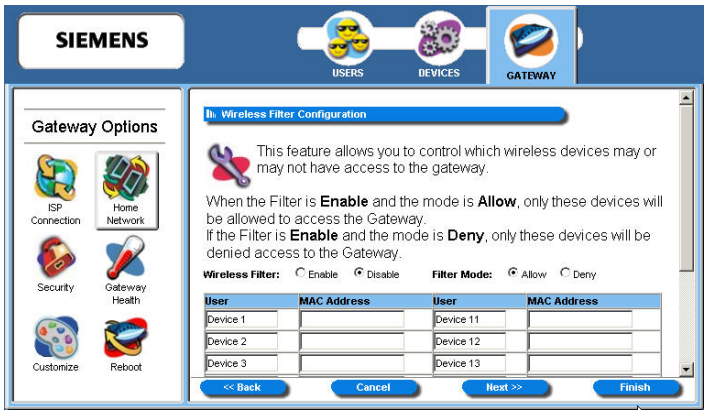
To use the WPA option:

1. From the "Wireless Security Configuration" window, select **WPA PSK** from the **Security Mode** drop-down menu.
2. Click **Next**. This displays the "Wireless WPA Configuration" window.

3. Select one of the following from the **Algorithms** drop-down menu:
   - **TKIP**
     Temporal Key Integrity Protocol is a more powerful security protocol than WEP. This option verifies the security configuration after encryption keys are determined, synchronizes changing of the unicast encryption key for each frame, and determines a unique starting unicast encryption key for each pre-shared key authentication.
   - **AES**
     Advanced Encryption Standard) supports a private key algorithm that ranges from 128 to 256 bits.
4. Type a key in **Shared Key**. The shared key is used to generate a dynamic encryption key for Gateway security.
5. Type a numeric value (in seconds) in **Group Key Renewal** to specify time to lapse between changing the key. The minimum time value is 30.
6. Click **Next**. This displays the "Wireless Filter Configuration" window.

Wireless Filter and Options Configuration

Control access to the Gateway of wireless devices based on the MAC address of the device using the "Wireless Filter Configuration" window. A MAC (Media Access Control) address refers to a hardware address that uniquely identifies each device of a network. Refer to the user documentation for each device you wish to deny or allow access for a particular MAC address.



To configure the wireless filter:

1. Select one of the following **Wireless Filter** options:

   - **Enable**
     Enable wireless filtering.

   - **Disable**
     Disable wireless filtering. If wireless filtering is disabled, all devices have access to the Gateway.

2. If wireless filtering is enabled, select one of the following **Filter Mode** options:

   - **Allow**
     Permits access to all the MAC addresses entered in the table.

   - **Deny**
     Restricts Gateway access to all the MAC addresses entered in the table.

3. Type the MAC address in the **MAC Address** column next to each device you either want to permit or restrict access.

4. Click **Next**. This displays the "Wireless Options Configuration" window.

5. Optionally, configure the following items:

   - **Data Transfer Rate**
     If a particular wireless client is unable to auto-negotiate a connection to the Gateway, the data transfer rate may be set to a specific data rate such as 11 Mbps for 802.11b wireless clients.
   - **RTS/CTS Threshold**
     A group of wireless clients may experience difficulty communicating with the Gateway without interrupting each other's communications. If this occurs, the RTS/CTS threshold may be set to a higher number to allow them each a longer period in which to communicate with the Gateway before the priority is switched to another wireless client wishing to transmit data.
   - **Fragmentation Threshold**
     The fragmentation threshold may be lowered to improve reliability in an excessively "noisy" wireless environment if changing channels does not provide significant enough improvement.

If you wish to reset the options in the "Wireless Options Configuration" window, click **Restore Default Values**. The system responds by restoring all the advanced features on this page.

6. Click **Next**. This displays the "Wireless Wizard" finish window.
7. Click **Finish** to save the settings.
8. Click **Reboot** for your wireless configuration to take effect.

Powerline Security Configuration

If you have a Powerline enabled Gateway, you have the option of configuring security for the Powerline connection.

To configure powerline security:

1. Select one of the following **Powerline Interface** options:

   - **Enable**
     Enables a powerline connection.
   - **Disable**
     Disables a powerline connection. Click **Next**. This displays the "Finish" window.

2. If you selected **Enable**, enter a password to secure your powerline connection. This password must be identical on all powerline client devices.

3. Select one the following from the **Security Level** drop-down menu.

   - **Off**
     Powerline encryption is turned off.
   - **Minimum**
     Data transmitted is encrypted. Receives all data: unencrypted and encrypted.
   - **Standard**
     Data transmitted is encrypted. Data received must be encrypted.
   - **Maximum**
     Same as standard. Data transmitted is encrypted. Data received must be encrypted.

4. Click **Next**. This displays the "Powerline Filter Configuration" window.

5. Select one of the following **Powerline Filter** options:

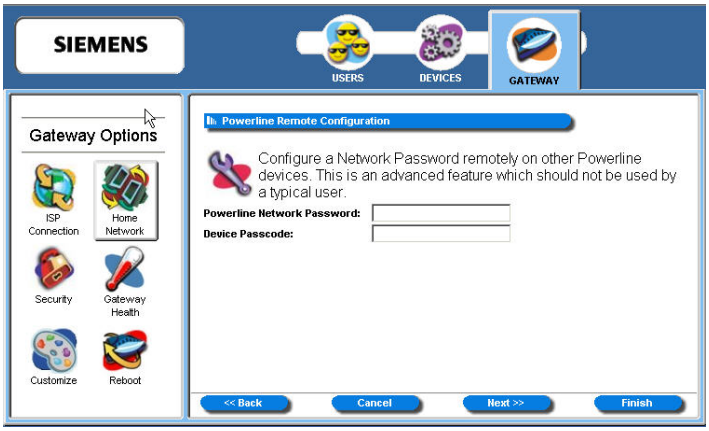
   - **Enable**
     Enables powerline filtering.
   - **Disable**
     Disables powerline filtering. If powerline filtering is disabled, all devices have access to the Gateway.

6. If powerline filtering is enabled, select one of the following **Filter Mode** options:

   - **Allow**
     Permits access to all the MAC addresses entered in the table.
   - **Deny**
     Restricts access to all the MAC addresses entered in the table.

7. Type the MAC address in the **MAC Address** column next to each device you either want to permit or restrict access.

8. Click **Next**. This displays the "Powerline Remote Configuration" window.



Optionally configure a network password remotely on other powerline devices. To do this:

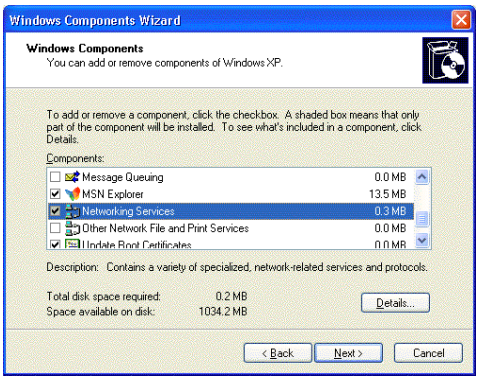
9. Enter the password you want to assign to all powerline devices in **Powerline Network Password**.
10. Enter the current password in **Device Password** for the powerline devices you want to change.
11. Click **Next**. This displays the Wizard "Finish" window.
12. Click **Reboot** to save the settings.

UPnP (Universal Plug and Play)

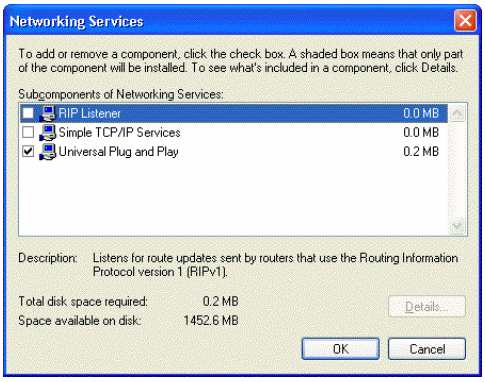
Microsoft UPnP allows the Gateway to communicate directly with certain Windows operating systems to trade information about the special needs of certain applications (such as messaging programs and interactive games) as well as provide information about other devices on the network. This communication between the operating system and Gateway greatly reduces the amount of manual configuration required to use new applications and devices.

Only certain versions of Windows XP and computer support the UPnP (Universal Plug and Play) function. Before configuring this option, make sure that UPnP is installed on your computer and enabled. Follow the steps below for installing UPnP components.

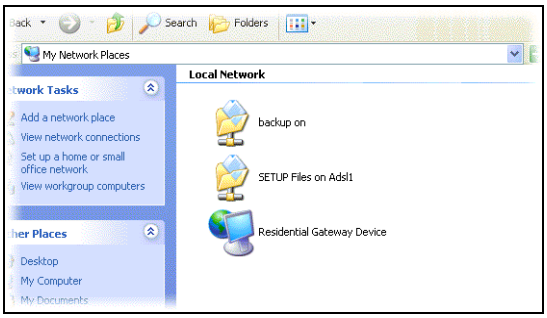
1. Select **Start>Control Panel**.
2. Select **Add or Remove Programs>Add/Remove Windows Components** to open the "Windows Components Wizard" window**.**


Windows Components Wizard
Windows Components
You can add or remove components of Windows XP.
To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
Message Queuing 0.0 MB
MSN Explorer 13.5 MB
Networking Services 0.3 MB
Other Network File and Print Services 0.0 MB
Update Root Certificates 0.0 MB
Description: Contains a variety of specialized, network-related services and protocols.
Total disk space required: 0.2 MB
Space available on disk: 1034.2 MB
Details...
< Back
Next >
Cancel

3. Select **Network Services** and click **Details**. This displays the "Networking Services" window.


Networking Services
To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Subcomponents of Networking Services:
RIP Listener 0.0 MB
Simple TCP/IP Services 0.0 MB
Universal Plug and Play 0.2 MB
Description: Listens for route updates sent by routers that use the Routing Information Protocol version 1 (RIPv1).
Total disk space required: 0.2 MB
Space available on disk: 1452.6 MB
Details...
OK
Cancel

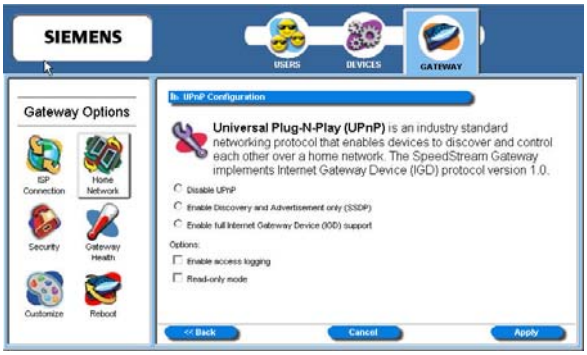
4. Select **Universal Plug and Play**.
5. Click **OK**. The system installs the UPnP components automatically.
6. After finishing the installation, go to **My Network Places**. You will find an icon for the UPnP function called Residential Gateway Device.



7. Double-click the icon. The Gateway will open another Web page for UPnP functions. Now, NAT functionality is available. The Gateway will create virtual servers automatically when it detects the computer running Internet applications that require this configuration.

Now you can configure the Gateway for UPnP. To configure UPnP on the Gateway:

1. Click **Configure the Universal Plug and Play Settings** link to display the "UPnP Configuration" window:



2. Select one of the following operating modes to enable or disable UPnP.

   - **Disable UPnP**
     Prevents the Gateway from using the UPnP feature to communicate with other devices or your operating system. Also may be disabled if your operating system does not support UPnP.
   - **Enable Discovery and Advertisement only (SSDP)**
     Sends information about new devices (hardware) detected only. No information concerning software applications or services is transmitted.
   - **Enable full Internet Gateway Device (IGD) support**
     Allows the Gateway to communicate freely with computers on the network about new devices, software applications, and services as needed to ensure they are working with minimal manual configuration required.

3. Select one of the following control options.

   - **Enable Access Logging**
     Logs UPnP transactions to the system log.
   - **Read Only Mode**
     Can read configuration information from a device; cannot modify the device configuration.

4. Click **Apply** to accept the settings. This displays the UPnP finish window.
5. Click **Reboot**.

Security

Your Gateway provides broad security measures against unwanted users. Security also allows for the configuration of the Gateway firewall, administrator password, (NAT) Network Address Translation, and DMZ (Demilitarized Zone) configuration.

To use the security option, click the **Security** button on the **Gateway Options** pane. This displays the "Security Options" window containing icons to access the security features.

This section is organized into parts that correspond to the following buttons shown in the **Gateway Option**s pane.

Configure the network firewall. A firewall is a system designed to prevent unauthorized access to or from a private network.

Change administrative password.

Configure address translation. Address translation hides individual users/computers behind a single outward-facing address. Hiding internal addresses allows greater security for your network.

Firewall Settings

A firewall is a system designed to prevent unauthorized access to or from a private network. The firewall window provides a listing of options to be enabled or disabled as well as links to configure the more complex details of each feature.

To configure the firewall:

1. From the "Security Options" window, click **Firewall Settings**. This displays the "Firewall Settings" window.

2. Select the checkboxes for all **Security** options you wish to enable. This can be any of the following:

   - **Level**
     Enable security level access is from the Gateway to the Internet or other networks. Click **Configure** to configure Security Level feature. This displays the "Firewall Level Configuration" window.

   - **Attack Detection**
     Enable protection from common hacker attacks to your computer/network from the Internet. Click **Configure** to configure the Attack Detection feature. This displays the "Attack Detection Configuration" window.

   - **IP Filtering**
     Configure inbound and outbound filter rules if your firewall Level setting is Custom. Click **Configure** to configure IP filter rules. This displays the "Firewall IP Filter Configuration Wizard" window.

3. Select **DMZ** for the **Gaming** option if you want to enable DMZ. Click **Configure** to configure firewall DMZ option. This displays the "Firewall DMZ Configuration" window.

4. Select the checkboxes for all **Support** options you wish to enable. This can be any of the following:

   - **Firewall Snooze Control**
     Bypass the firewall for a set amount of time so outside support personnel can access your Gateway or network or so you can run an application that conflicts with the firewall. Click Configure to configure the snooze control. This displays the "Firewall Snooze Control" window.

Security Level

Security level refers to how much access is permitted from your Gateway to the Internet or other networks.

To enable and configure the security level feature:

1. Select **Level** from the "Firewall Settings" window.
2. Click the **Configure** hyperlink next to **Level**. This displays the "Firewall Level Configuration" window.

SIEMENS
USERS
DEVICES
GATEWAY
Gateway Options
ISP Connection
Home Network
Security
Gateway Health
Customize
Reboot
Your SpeedStream Gateway supports various Security Levels to match your security needs.
Level
Description
Off
Data traffic flows in and out without any firewall protection.
Low
Attack Detection is enabled and well-known ports are still available for traffic to pass through to the Internet.
High
Only certain applications are allowed through the firewall or traffic that is already "in conversation" with an application from the host PC and host application. ICSA 3.0a Compliant.
Custom
Custom rules can be applied using the IP Filtering option under Firewall.
Select Firewall Level
Low
<< Back
Cancel
Apply

3. Select the firewall security level from the **Select Firewall Level** drop-down menu. This can be one of the following:

   - **Off**
     No firewall protection. Data can move freely both in and out of the Gateway.
   - **Low**
     Provides basic firewall protection. Attack detection is enabled and only ports well known to the Gateway can allow the flow of data.
   - **High**
     Provides maximum firewall protection. Only certain applications are allowed through the firewall or traffic that is already "in conversation" with an application from the host PC and host application. (ICSA 3.0a Compliant.)
   - **Custom**
     Set your own rules for firewall protection. This option should be used by advanced users only. If you select this option, you must set customized rules for both inbound and outbound traffic using the IP Filtering option.

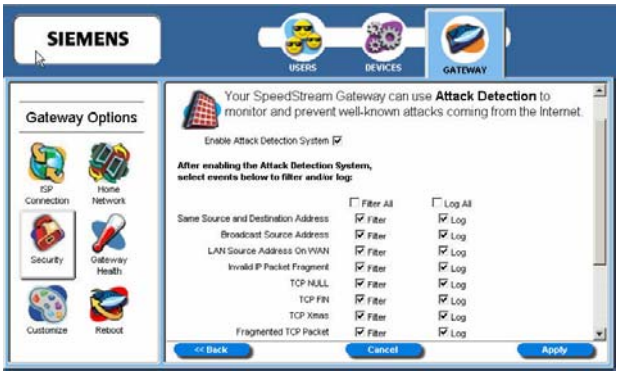
4. Click **Apply**.

Attack Detection

If the Attack Detection System is enabled, the Gateway provides protection against the most common hacker attacks that attempt to access your computer/network from the Internet. Intrusion attempts can also be logged to provide a record of attempts and their source (when available).

To enable and configure the attack detection feature:

1. Select **Attack Detection** from the "Firewall Settings" window.
2. Click the **Configure** hyperlink next to **Attack Detection** option. This displays the "Attack Detection Configuration" window.



3. Select **Enable Attack Detection**.
4. Select **Filter** for each event in the list you want to filter or, if you want to filter all events, select **Filter All**. This provides maximum protection against malicious intrusion from outside your network.
5. Select **Log** for each event in the list you want to log or, if you want to log all events, select **Log All**.
6. Click **Apply**.

Below is a description of each event that can be monitored.

- **Same Source and Destination Address**
  An outside device can send a SYN (synchronize) packet to a host with the same source and destination address (including port) causing the system to hang. When the receiving host tries to respond to the source address in the packet, it ends up just sending it back to itself. This packet could ping-pong back and forth over 200 times (consuming CPU resources) before being discarded.
- **Broadcast Source Address**
  An outside device can send a ping to your Gateway broadcast address using a forged source address. When your system responds to these pings, it is brought down by echo replies.
- **LAN Source Address on LAN**
  An outside device can send a forged source address in an incoming IP packet to block trace back.
- **Invalid IP Packet Fragment**
  An outside device can send fragmented data packets that can bring down your system. IP packets can be fairly large in size. If a link between two hosts transporting a packet can only handle smaller packets, the large packet may be split (or fragmented) into smaller ones. When the packet fragments get to the destination host, they must be reassembled into the original large packet like pieces of a puzzle. A specially crafted invalid fragment can cause the host to crash
- **TCP NULL**
  An outside device can send an IP packet with the protocol field set to TCP but with an all null TCP header and data section. If your Gateway responds to this attack, it will bring down your system.

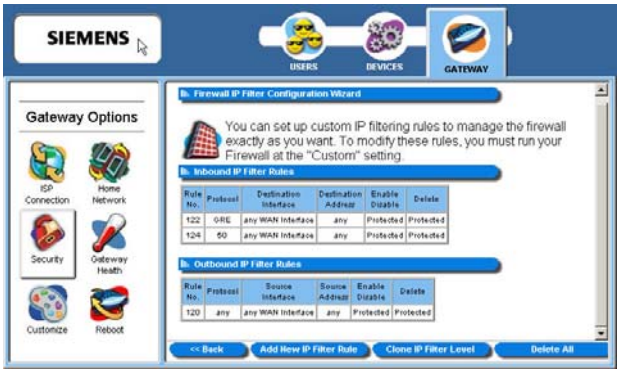
- **TCP FIN**
  An outside device can send an attack using TCP FIN. This attack never allows a data packet to finish transmitting and brings down your system.
- **TCP XMAS**
  An outside device can send an attack using TCP packets with all the flags set. This causes your system to slow to a halt.
- **Fragmented TCP Packet**
  An outside device can send an attack using fragmented packets to allow an outside user Telnet access to a device on your network.
- **Fragmented TCP Header**
  An outside device can send an attack using TCP packets with only a header and no payload. When numerous packets are sent through the Gateway in this manner, your system slows and halts.
- **Fragmented UDP Header**
  An outside device can send an attack using fragmented UDP headers to bring down a device on your network.
- **Fragmented ICMP Header**
  An outside device can send an attack using fragmented ICMP headers to bring down a device on your network.
- **Inconsistent UDP/IP header lengths**
  An outside device can send an attack using inconsistent UDP/IP headers to bring down a device on your network.
- **Inconsistent IP header lengths**
  An outside device can send an attack using changes in the IP header to zero the fragment offset field. This will be treated as a complete packet when received and cause your system to halt.

IP Filtering

Define inbound and outbound IP filter rules using this procedure. IP filtering rules can only be defined if the **Firewall Level** setting is **Custom**. This method of firewall protection is recommended for advanced users only.

To define IP filtering rules:

1. Click the **Configuration** hyperlink next to the **IP Filter** option on the "Firewall Settings" window. This displays the "Firewall IP Filter Configuration Wizard" window.



2. Do one of the following:

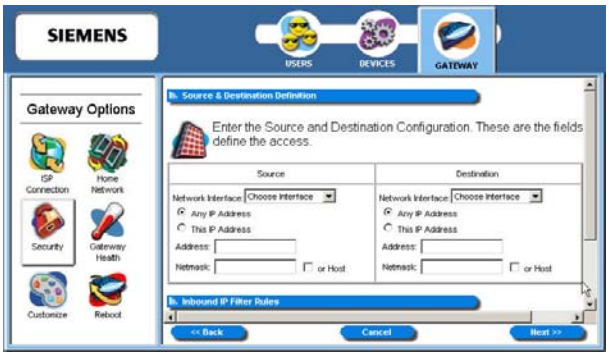
   - Click **Add New IP Filter Rule** to add new IP filter rules. This displays the "Basic Rule Definition" window.
   - Click **Clone IP Filter Level** to clone IP filter rules already defined. This displays the "Clone Rule Definition" window. Once cloned, you can modify the existing rules.

Add New IP Filter Rules

The "Basic Rule Definition" window is displayed when you select **Add New IP Filter Rule** from the "Firewall IP Configuration Wizard" window. Using this option, you can define both inbound and outbound rules. Each rule defined is added to the Rule Definition table.

To add a new rule:

1. Type up to a five digit numeric value in **Rule No** to uniquely identify the rule.
2. Select either **Permit** or **Deny** from the **Access** drop-down menu. Select **Permit** to allow the rule and **Deny** to prohibit the rule.
3. Select either **Inbound** or **Outbound** from the **Direction** drop-down menu. **Inbound** refers to data coming into the Gateway, while **Outbound** refers to data transmitted from the Gateway.
4. Optionally, select **Disable stateful inspection for packets matching this rule**.
5. Optionally, select **Create a log entry for packets matching this rule**. When selected, an entry is placed in the log file when packets match this rule.
6. Click **Next**. This displays the "Source and Destination Definition" window.



7. Under the **Source** heading, select a network connection from the **Network Interface** drop-down menu.
8. Select one of the following options:

   - **Any IP Address**
     Select this option if this rule applies to any IP address from the source.
   - **This IP Address**
     Select this option if a rule applies to a specific IP address from the source.

9. If you selected **This IP Address**, enter an IP address in the **IP Address** field and do one of the following:
   - Enter a netmask in the **Netmask** field.
   - Select **or Host** to use your Gateway netmask as the source netmask.
10. Under the **Destination** heading, select a network connection from the **Network Interface** drop-down menu.
11. Select one of the following options:
    - **Any IP Address**
      Select this option if this rule applies to any IP address of the destination.
    - **This IP Address**
      Select this option if a rule applies to a specific IP address of the destination.
12. If you selected **This IP Address**, enter an IP address in the **IP Address** field and do one of the following:
    - Enter a netmask in the **Netmask** field.
    - Select **or Host** to use your Gateway netmask as the destination netmask.
13. Click **Next**. This displays the "Protocol Definition" window.

14. Do one of the following:
    - Select one of the following protocol options from the **Select by Name** drop-down menu. This defines the types of packets filtered.
      - Any Protocol
      - TCP (Transmission Control Protocol):
        Provides reliable, sequenced, and unduplicated delivery of bytes to remote or local users. Click Next to display the "TCP/UDP Options" window.
      - UDP (User Datagram Protocol):
        Provides for the exchange of datagrams without acknowledgement or guaranteed delivery. Click Next to display the "TCP/UDP Options" window.
      - **ICMP** (Internet Control Message Protocol):
        A mechanism that provides for peer communication. The most commonly used application for this protocol is the PING command. Click **Next** to display the "ICMP Options" window.
      - **GRE** (Generic Routing Encapsulation):
        A tunneling protocol that is used primarily for VPN (Virtual Private Networks).
    - Type a protocol number in the **Select by Number** field.
15. Click **Finish**.

TCP/UDP Options Window

The "TCP/UDP Options" window is displayed if you select TCP or UDP protocol from the "Protocol Definition" window. If you selected either of these protocol types, you must identify the source and destination ports.

1. Select one of the following options from the **Source Port Operator** drop-down menu and the **Destination Port Operator** drop-down menu:

   - **any**
     Any port is acceptable as the source/destination port.
   - **less than or equal to**
     A port less than or equal to the numeric value in the **Port 1** field is acceptable as the source/destination port. Be sure to provide a value in the **Port 1** field.
   - **equal to**
     A port equal to the numeric value in the **Port 1** field is acceptable as the source/destination port. Be sure to provide a value in the **Port 1** field.
   - **greater than or equal to**
     a port greater than or equal to the numeric value in the **Port 1** field is acceptable as the source/destination port. Be sure to provide a value in the **Port 1** field.
   - **range**
     Any port between the value of the entry in the **Port 1** field and the value in the **Port 2** field is acceptable as the source/destination port. Be sure to provide a value in the **Port 1** and **Port 2** fields.

2. Optionally, select **Check TCP syn packets** if you wish this rule to prevent the blocking of synchronization packets for pre-existing sessions.
3. Click **Next**.
4. Click **Finish**.

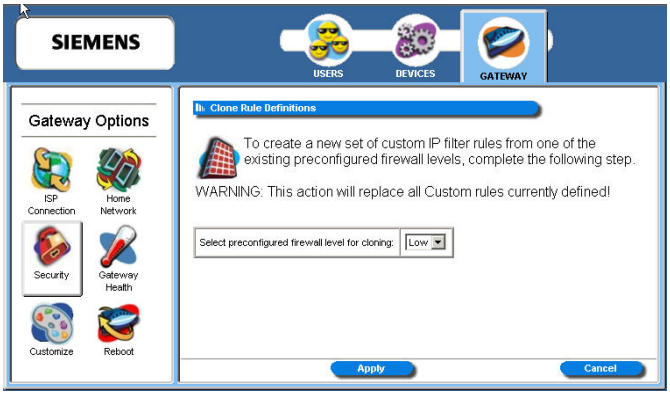
ICMP Options Window

The "ICMP Options" window is displayed if you select ICMP protocol from the "Protocol Definition" window.

1. Do one of the following:
   - Select any of the ICMP options you wish to filter.
   - Select **All Types** to filter all options.
2. Click **Next**.
3. Click **Finish**.

Clone IP Filter Rules

The "Clone Rule Definitions" window is displayed when you select **Clone IP Filter Level** from the "Firewall IP Configuration Wizard" window. Using this option, you can clone either high or low level rules and modify them according to your needs. If you choose to clone IP filter rules, the rules already defined in the Rule Definition table are discarded.



To clone IP filter rules:

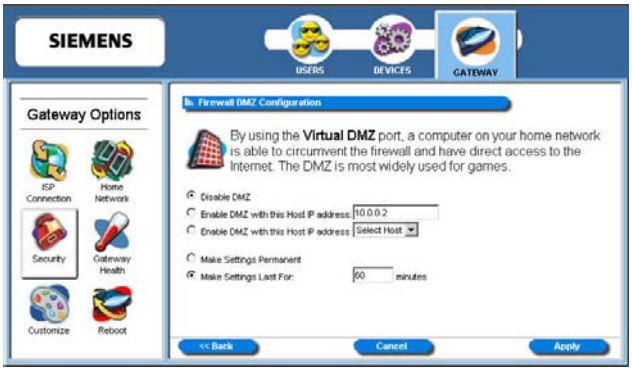
1. Select one of the following from the **Select preconfigured firewall level for cloning** drop-down menu.
   - **Low**
     Clones low-level IP filter rules.
   - **High**
     Clones high-level IP filter rules.
2. Click **Apply**. This displays the "Firewall IP Filter Configuration Wizard" window with the selected rule set showing in the Rule Definition table.
3. Disable or delete any rule as desired.

DMZ

The DMZ feature allows a computer on your home network to circumvent the firewall and have direct access to the internet. This feature is primarily used for gaming. The Gateway allows you to configure a temporary or permanent DMZ (Demilitarized Zone) to bypass the firewall for network or Internet gaming. If the DMZ feature is enabled, you must select the computer to be used as the DMZ computer/host. This function is recommended for use only when you require this special level of unrestricted access as it leaves your Gateway and network exposed to the Internet with no firewall protection.

To enable and configure the DMZ:

1. Select **DMZ** from the "Firewall Settings" window.
2. Click the **Configure** hyperlink next to **DMZ**. This displays the "Firewall DMZ Configuration" window.


SIEMENS
USERS
DEVICES
GATEWAY
Gateway Options
ISP Connection
Home Network
Security
Gateway Health
Customize
Reboot
Firewall DMZ Configuration
By using the Virtual DMZ port, a computer on your home network is able to circumvent the firewall and have direct access to the Internet. The DMZ is most widely used for games.
Disable DMZ
Enable DMZ with this Host IP address: 10.0.0.2
Enable DMZ with this Host IP address: Select Host
Make Settings Permanent
Make Settings Last For: 60 minutes
<< Back
Cancel
Apply

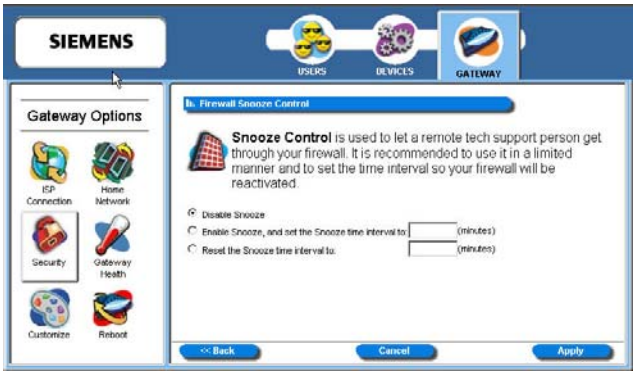
3. Select one of the following DMZ enable options:
   - **Disable DMZ**
     The firewall is not bypassed.
   - **Enable DMZ with this Host IP address**
     The firewall is bypassed through an IP address typed in the box next to this field.
   - **Enable DMZ with this Host IP address**
     The firewall is bypassed through an IP address that is selected from the **Select Host** drop-down menu next to this field. Select the desired host from the drop down.
4. Select one of the following time element options:
   - **Make Settings Permanent**
     DMZ settings are permanent unless changed by the administrator.
   - **Make Settings Last for**
     DMZ settings last for only the time (in minutes) entered in the box next to this option.
5. Click **Apply**.

Firewall Snooze Control

The snooze feature allows you to bypass the firewall for a set amount of time so outside support personnel can access your Gateway or network, or so you can run an application that conflicts with the firewall. This function is recommended for use only when you require this special level of unrestricted access as it leaves your Gateway and network exposed to the Internet with no firewall protection.

To enable and configure snooze control:

1. Select **Firewall Snooze Control** from the "Firewall Settings" window.
2. Click the **Configure** hyperlink next to **Firewall Snooze Control**. This displays the "Firewall Snooze Control" window.



3. Select one of the following options:
   - **Disable Snooze**
     Disables all snooze control. In this mode, the firewall is not bypassed.
   - **Enable Snooze, and set the Snooze time interval to**
     Enables snooze for a specified time period. Be sure to enter the number of minutes to define how long the firewall should be disabled.
   - **Reset the Snooze time interval to**
     Reset the snooze control time period. Use this option if you need a time extension for an open snooze session. Be sure to specify the additional amount of time (minutes) the firewall should be disabled.
4. Click **Apply**.

Administrator Password

You may change the Gateway administrator password at any time if you have administrative rights to the Gateway. To change the administrator password:

1. From the "Security Options" window, click the **Admin Password** button. This displays the "Enter Network Password" window.
2. Provide the administrator log on ID and password, then click **OK**. This displays the Gateway Administrator Setup window.

SIEMENS
USERS
DEVICES
GATEWAY
Gateway Options
ISP Connection
Home Network
Security
Gateway Health
Customize
Reboot
h. Gateway Administrator Setup
Your Gateway requires someone to be the Gateway Administrator. This person has responsibility for adding user profiles, setting each person's access rights, and configuring the Gateway.
Please create a user name and password for the Gateway administrator.
Please enter unique information to configure the SpeedStream DSL Gateway:
User Name: admin (required)
New Password: ****** (required)
Confirm Password: ****** (required)
<< Back
Save Settings

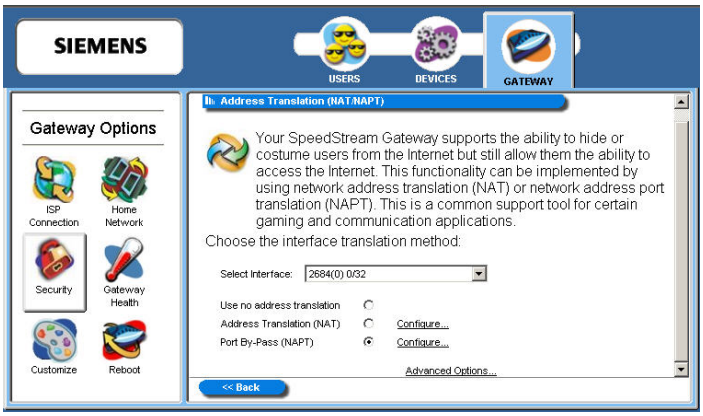
3. Make any desired changes to the **User Name**, **New Password**, and **Confirm Password**.
4. Click **Save Settings**.

Address Translation

The Address Translation feature provides different methods of keeping individual users/computers hidden behind a single outward-facing address, while still allowing them to access the Internet and related applications. If you have more than one available Internet connection interface, they will all be displayed in the drop-down menu for ease of selection.

To enable and configure the address translation feature:

1. From the "Security Options" window, select the **Address Translation** button. This displays the "Address Translation (NAT/NAPT)" window.


SIEMENS
USERS
DEVICES
GATEWAY
Gateway Options
ISP Connection
Home Network
Security
Gateway Health
Customize
Reboot
Address Translation (NAT/NAPT)
Your SpeedStream Gateway supports the ability to hide or costume users from the Internet but still allow them the ability to access the Internet. This functionality can be implemented by using network address translation (NAT) or network address port translation (NAPT). This is a common support tool for certain gaming and communication applications.
Choose the interface translation method:
Select Interface: 2684(0) 0/32
Use no address translation
Address Translation (NAT) Configure...
Port By-Pass (NAPT) Configure...
Advanced Options...
<< Back

2. Select an interface from the **Select Interface** drop-down menu.
3. Select one of the following options:

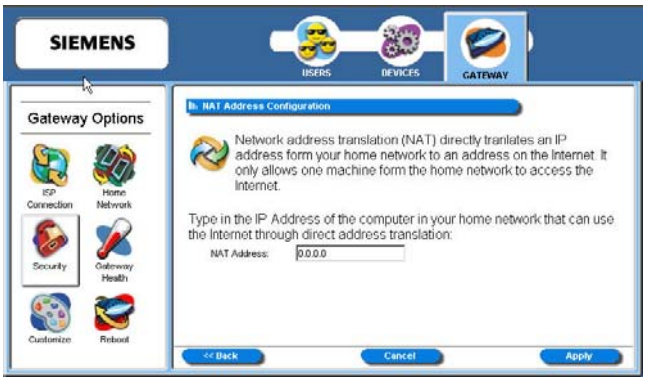
   - **Use no address translation**
     Disables address translation.
   - **Address Translation (NAT)**
     Uses NAT for address translation. NAT is an Internet standard that allows a LAN to use one set of IP addresses for internal traffic and a second set for external traffic. This displays the "NAT Address Configuration" window.
   - **Port By-Pass (NAPT)**
     Uses NAPT for address translation. Only TCP, UDP, and ICMP protocols support NAPT. NAPT allows many devices connected to the Gateway access to the Internet while masking the identification of the internal IP addresses. This displays the "Port By-Bass Configuration" window.

Address Translation With NAT

Network Address Translation (NAT) translates an IP address from your home network to an address on the Internet. It allows only one machine to access the Internet.

To enable and configure NAT address translation:

1. Select **Address Translation (NAT)** from the "Address Translation (NAT/NAPT)" window.
2. Click the **Configure** hyperlink next to **Address Translation (NAT)**. This displays the "NAT Address Configuration" window.


SIEMENS
USERS
DEVICES
GATEWAY
Gateway Options
ISP Connection
Home Network
Security
Gateway Health
Customize
Reboot
NAT Address Configuration
Network address translation (NAT) directly tranlates an IP address form your home network to an address on the Internet. It only allows one machine form the home network to access the Internet.
Type in the IP Address of the computer in your home network that can use the Internet through direct address translation:
NAT Address:
0.0.0.0
<< Back
Cancel
Apply

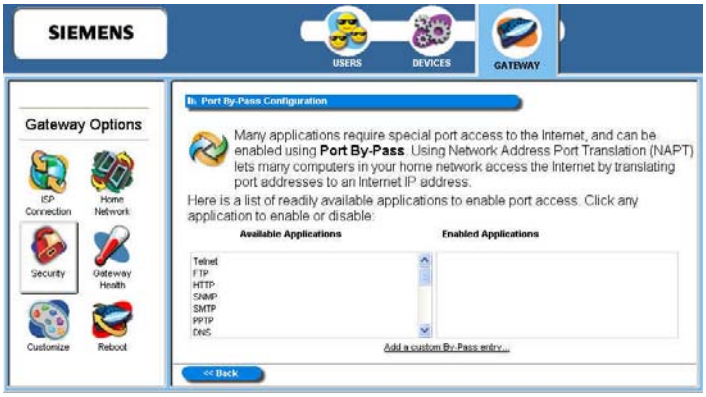
3. Type the IP address of the one computer in your network that you wish to have access to the Internet.
4. Click **Apply**.

Address Translation With NAPT

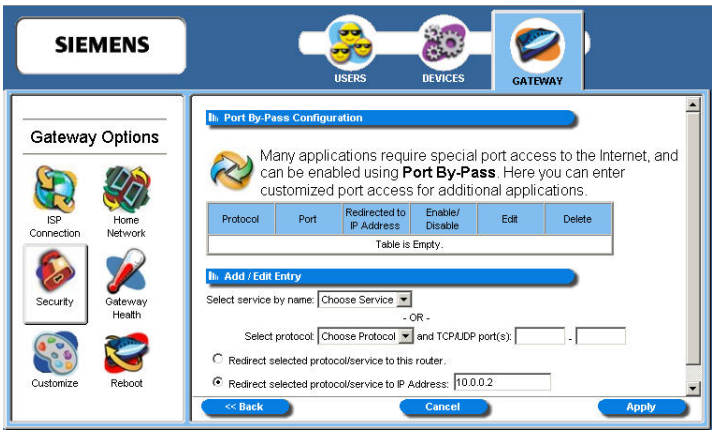
Many applications require special port access to the Internet in order to function. By enabling Network Address Port Translation (NAPT), multiple computers in your home network have access to the Internet by translating port addresses to an Internet IP address while masking their IP addresses from outside users. Only TCP, UDP, and ICMP protocols support NAPT.

To enable and configure NAPT address translation:

1. Select **Port By-Pass (NAPT)** from the "Address Translation (NAT/NAPT)" window.
2. Click the **Configure** hyperlink next to **Port By-Pass (NAPT)**. This displays the "Port-By-Pass Configuration" window.



3. To enable an application for NAPT, click the desired application from the **Available Applications** list. The application is moved to the **Enabled Applications** list.
4. Optionally, click the **Add a custom bypass entry** hyperlink. This displays the advanced features on the Port By-Pass Configuration" window. The advanced option allows you to configure special port access to the Internet.



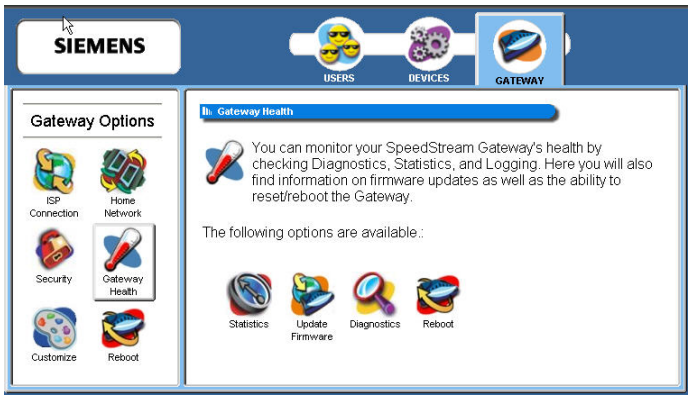
5. Do one of the following:
   - Select one of the following services from the **Select service by name** drop-down menu.
     - **Telnet**
       Telnet is a program that allows you to connect to other computers over the Internet. This options uses port 23.
     - **FTP** (File Transfer Protocol)
       FTP is used to transfer files in both ASCI and Binary format between local and remote devices. This option uses port 21.
     - **HTTP** (Hyper Text Transfer Protocol)
       HTTP is the standard method of transferring all types of information over the Internet. This option uses port 80.
     - **SNMP** (Signaling Network Management Protocol)
       SNMP is a protocol used by network management applications to help manage a network. This option uses port 161.
     - **SMTP** (Simple Mail Transfer Protocol)
       SMTP is used for sending email between servers. This port uses port 25.
     - **PPTP** (Point-to-Point Tunneling Protocol)
       PPTP is a protocol that allows VPN (Virtual Private Network) applications. This option uses port 1723.
     - **Domain**
       Domain is used for DNS options. This option uses port 53.
   - Select a protocol from the **Select Protocol** drop-down menu. This can be one of the following:
     - **TCP** (Transmission Control Protocol)
       Provides reliable, sequenced, and unduplicated delivery of bytes to a remote or local user.
     - **UDP** (User Datagram Protocol)
       A connectionless mode protocol that provides the delivery of packets to a remote or local user.
     - **ICMP** (Internet Control Message Protocol)
       A method by which IP software on a host or Gateway can communicate to pass information to other machines.
     - **GRE** (Generic Routing Encapsulation)
       This protocol is used to provide tunneling for a VPN connection.
6. If you selected a protocol, type the range of UDP or TCP ports in the appropriate boxes
7. Select one of the following options:
   - **Redirect selected protocol/service to this router**
     The protocol or service that you select is directed to your Gateway.
   - **Redirect selected protocol/service to IP Address**
     The protocol or service that you select is directed to an IP address on your LAN that you type in the box next to this field.
8. Click **Apply**.

Chapter 7

Monitoring Gateway Health

This chapter explains how to monitor the health of the Gateway.

This chapter describes how to monitor the health of the Gateway. The Gateway health options are used to gauge the various measures of Gateway's health. To use the Gateway health options, click the **Gateway Health** button from the **Gateway Options** pane. This displays the "Gateway Health" window.



Gateway Health options discussed in this chapter:

This chapter is organized into parts that correspond to the following buttons shown in the **Gateway Health** pane.

Statistics

Used to measure the Internet stats, home networking stats, security stats, and the different Gateway log files.

Update Firmware

Updates the firmware of your Gateway through the Internet or from a device connected to your Gateway. (Not all Gateways will have this option.)

Diagnostics

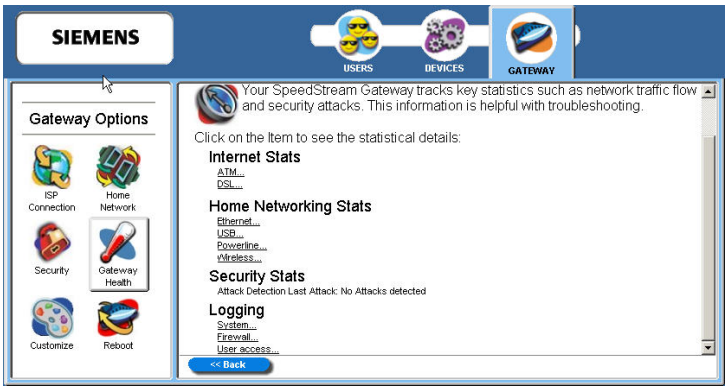
Runs a diagnostic program against a selected connection on your Gateway.

Reboot

Reboots the system or resets all settings to Gateway factory defaults.

Statistics

You can display statistics for the Internet, Home Networking, Security, and Logging. To display any of these statistics, click the **Statistics** button from the "Gateway Health" window. This displays the "SpeedStream Gateway Statistics" window.



Click the hyperlink for the type of statistics you wish to view. These fall into four categories:

- **Internet Stats**
  Internet statistics are commonly used by your Internet Service provider to diagnose service-related issues. Internet statistics include either ATM or DSL statistics.
- **Home Networking Stats**
  Home Networking statistics are helpful for troubleshooting issues on your home network. These statistics are displayed for each physical interface connected to the Gateway. They are separated into Ethernet, USB, Powerline, or Wireless statistics.
- **Security Stats**
  Security breach attempts are shown for any firewall rules or attack detection services you have defined on the Firewall customization window.
- **Logging**
  Extensive activity logs are provided for advanced troubleshooting and administrative use. The following types of logs are available: System, Firewall, and User Access.

Internet Stats

Internet statistics are commonly used by your Internet Service provider to diagnose service-related issues. Internet statistics include either ATM or DSL statistics.

ATM Statistics

View status and statistical information for the WAN-side Asynchronous Transfer Mode (ATM) network connection. WAN-side connection to the service provider is based on an Asynchronous Transfer Mode (ATM) network connection. In addition, statistical information is provided for each Virtual Circuit (VC) configured under the ATM Adaptation Layer (AAL).

To view ATM statistics, click the **ATM** hyperlink under **Internet Stats**.

DSL Statistics

View status and statistical information for the Digital Subscriber Line (DSL) when the physical WAN-side connection to the service provider is achieved through a DSL line. Statistical information is accumulated over periodic intervals and may be displayed for up to a 24 hour period.

To view DSL statistics, click the **DSL** hyperlink under **Internet Stats**

Home Networking Stats

Home Networking statistics are helpful for troubleshooting issues on your home network. These statistics are displayed for each physical interface connected to the Gateway. They are separated into Ethernet, USB, Powerline, or Wireless statistics.

Ethernet Statistics

View status and statistical information for LAN-side Ethernet connectivity.

Pay special attention to the status (up or down) reported for each Ethernet port to verify that each cable is connected properly and detected by the Gateway.

USB Statistics

View status and statistical information for LAN-side USB connectivity.

Pay special attention to the status (up or down) reported for each USB port to verify that each cable is connected properly and detected by the Gateway.

Powerline Statistics

View status and statistical information for Powerline connectivity.

Pay special attention to the status (up or down) reported for the Powerline connection to verify that powerline is connected properly and detected by the Gateway.

Wireless Statistics

View status and statistical information for Wireless connectivity.

Pay special attention to the status (up or down) reported for the wireless connection to verify that the wireless connection is properly configured and detected by the Gateway.

Logging

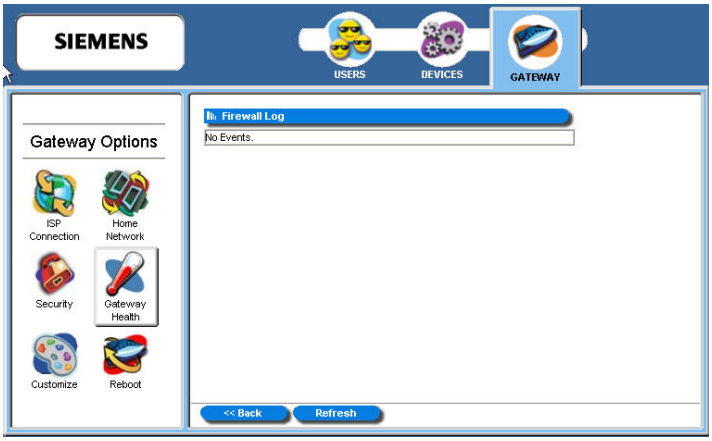
Extensive activity logs are provided for advanced troubleshooting and administrative use. The following types of logs are available: System, Firewall, and User Access.

System Logging

System logging displays Gateway status, user login, interfaces accessed, etc. Activity displayed in the system log is defined using the checkboxes provided at the bottom of the window. Click Apply after making any changes. The system log can be cleared or saved to a text file using the appropriate buttons, Clear Log or Save Log.

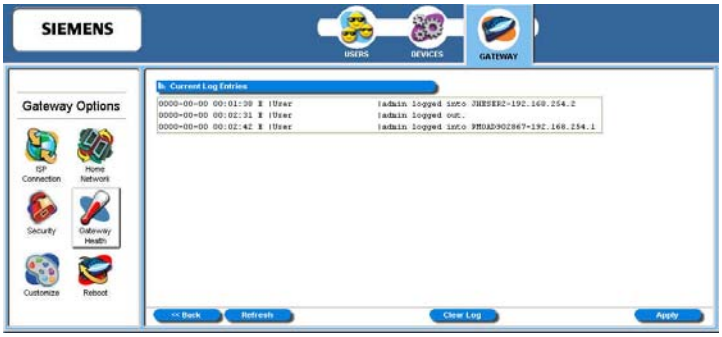
Firewall Logging

Firewall Logging displays attempts (both failures and successes) to access data through the firewall. Firewall log entries are defined on the **Firewall Settings Configuration** window found under the **Security** menu.



User Access

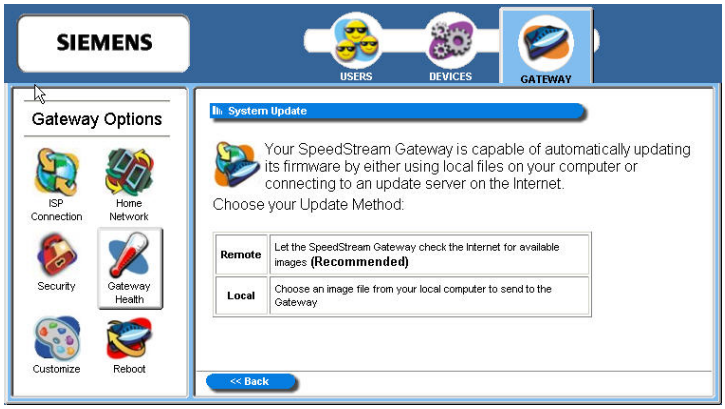
User Access logging displays activity related to users logging in or out of the Gateway. Both successful and unsuccessful attempts by username are recorded.



Update Firmware

This feature updates the firmware of your Gateway through the Internet or from a device connected to your Gateway. This option may not be available on your Gateway configuration. If available, you must be logged in as the Gateway Administrator to access the utility.

To access this feature, click the **Update Firmware** button from your "Gateway Health" window. This displays the "System Update" window.


SIEMENS
USERS
DEVICES
GATEWAY
Gateway Options
ISP Connection
Home Network
Security
Gateway Health
Customize
Reboot
System Update
Your SpeedStream Gateway is capable of automatically updating its firmware by either using local files on your computer or connecting to an update server on the Internet.
Choose your Update Method:
Remote
Let the SpeedStream Gateway check the Internet for available images (Recommended)
Local
Choose an image file from your local computer to send to the Gateway
<< Back

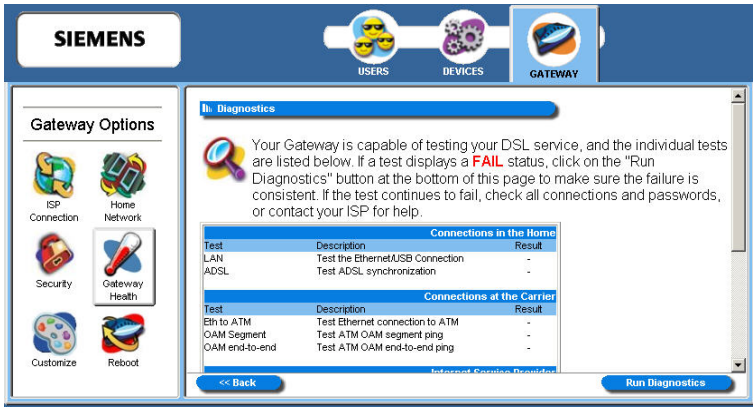
Select one of the following download options to start the download process.

- **Remote**
  Checks the Internet for the appropriate upgrade file. This is the recommended method.
- **Local**
  Download the firmware update from a location on your network and select the upgrade file. Before doing this, you must download the upgrade file to your computer.

Important: Do not turn off or interrupt the Gateway during a firmware upgrade session. The Gateway could be rendered inoperable!

Diagnostics

The Gateway provides diagnostic tests and data for each interface. This data is commonly requested by technical support to assist in troubleshooting. To access this feature, click the **Diagnostics** button from your "Gateway Health" window. This displays the "Diagnostics" window.


SIEMENS
USERS
DEVICES
GATEWAY
Gateway Options
ISP Connection
Home Network
Security
Gateway Health
Customize
Reboot
Diagnostics
Your Gateway is capable of testing your DSL service, and the individual tests are listed below. If a test displays a FAIL status, click on the "Run Diagnostics" button at the bottom of this page to make sure the failure is consistent. If the test continues to fail, check all connections and passwords, or contact your ISP for help.
Connections in the Home
Test Description Result
LAN Test the Ethernet/USB Connection -
ADSL Test ADSL synchronization -
Connections at the Carrier
Test Description Result
Eth to ATM Test Ethernet connection to ATM -
OAM Segment Test ATM OAM segment ping -
OAM end-to-end Test ATM OAM end-to-end ping -
<< Back
Run Diagnostics

To use the diagnostic option:

1. Select a connection to test from the **Connection to Test** drop-down menu. You must move all the way to the bottom of this window to display this drop-down menu.
2. Click **Run Diagnostics**. The system responds by displaying the results in the different tables. Pay special attention to any tests that report a failing condition and check the connections for these interfaces before running the diagnostics again.
3. Click **Apply**.

Chapter 8

Miscellaneous Gateway Options

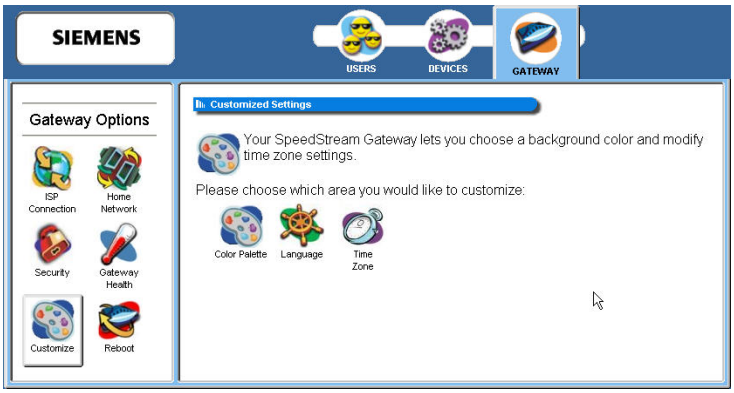
This chapter explains how to customize the appearance of the configuration program and to reboot the Gateway. This chapter is organized into parts that correspond to the following buttons shown in the **Gateway Options** pane.

Customize the Gateway's display.

Reboot the Gateway.

Customize

You are able to control the background color, language, and time zone settings of your Gateway using customization options. To access the customization options, click the **Customization** button from the **Gateway Options** pane. This displays the "Customized Settings" window.



Customization options discussed in this chapter:

Customize the appearance of the configuration interface/program.

Select language to display in text. (Not all Gateways will have this option.)

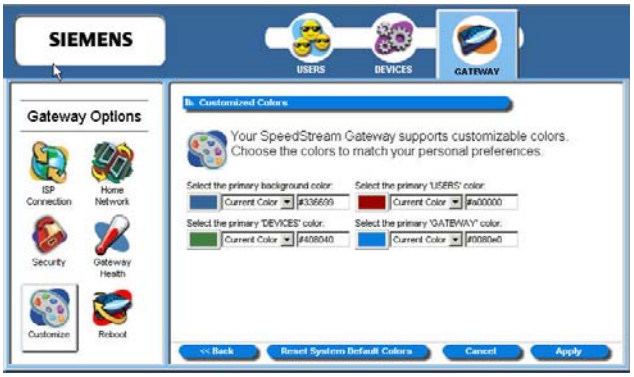
Configure time parameters to automatically synchronize the Gateway's internal date and time settings with those of your selected time zone.

Color Palette

Multiple color selections are available to customize the appearance of the configuration interface/program.

To configure the color palette:

1. From the "Customized Settings" window, click the **Color Palette** button. This displays the "Customized Colors" window.



2. Using the color drop-down menus from the different display options, select the colors you wish to use in the system.
3. Optionally, type a numeric color value in the box next to the particular color drop-down menu. The number is based on RGB (Red Green Blue) values. For example, the color red is represented by a value of ff0000, green is represented by a value of 00ff00, and blue is represented by a value of 0000ff. If you are entering a numeric value for the color, ensure that the "#" is in front of your numeric value.

   Click **Reset System Default Colors** if you want to reset all system color schemes to the factory settings.
4. Click **Apply**.

Language

Multiple languages may be available for displaying text in the configuration interface/program. This option may not be available on your Gateway configuration.

To set the language used on the Gateway windows:

1. From the "Customized Settings" window, click the **Language** button. This displays the "Customized Language" window.

2. Select your desired language.
3. Click **Apply**.

Time Zone

Using this option, you can configure the time parameters to automatically synchronize the Gateway's internal date and time settings with those of your selected time zone. This time will be used to control time restrictions you may set for users as well as in entries in the system log.

To enable and configure the time zone feature:

1. From the "Customized Settings" window, click the **Time Zone** button. This displays the "Configure Time Zone" window.

2. Select **Yes** for **Enable Time Client**.
3. Select a time zone from the **Select Time Zone** drop-down menu.

   Note: The Gateway's time server is unable to determine whether your time zone is currently observing daylight savings time. If you are currently observing daylight savings time, select an alternate time zone that matches your time settings during daylight savings time observation periods.
4. Click **Apply**.

Reboot

You can reboot the Gateway using the Reboot option, or you can reset the Gateway to factory defaults using the reset option. Reboot should be used when the Gateway needs to be restarted. The Gateway can also be rebooted using the power switch on the rear panel of the Gateway. This option can be used at either the user or administrator level.

To reboot or reset factory defaults on the Gateway:

1. Click the **Reboot** button from the **Gateway Options** pane. This displays the "System Reboot" window.

2. If you want the factory default settings to be reset, click **Reset to Factory Defaults**. Reset should be used when you find it necessary to recover the factory default settings. This may be necessary when a custom configuration did not go as planned, when a new configuration is desired, or when the Gateway does not appear to be working properly. This option resets all custom settings, users, and passwords on your Gateway. You must be logged on as the administrator to use this option.
3. Click **Reboot**.

Appendix A

Troubleshooting

Overview

This chapter covers some common problems that may be encountered while using the Wireless DSL Gateway and some possible solutions to them. If you follow the suggested steps and the Gateway still does not function properly, contact your Internet Service Provider or Technical Support for assistance.

General Issues

Problem: **Can't connect to the Gateway to configure it.**

Solution: Check the following:

- The Gateway is properly installed, connections are OK, and it is powered ON. Check the LEDs for Ethernet or USB port status.
- Ensure that your computer and the Gateway are on the same network segment.
- If your computer is set to "Obtain an IP Address automatically" (DHCP client), restart your computer.

Internet Access

Problem : **When I enter a Web site address or IP address I get a time out error.**

Solution: A number of things could be causing this. Try the following troubleshooting steps.

- Verify that other computers work. If they do, ensure that your computer's IP settings are correct. If using a fixed (static) IP address, check the network mask, default Gateway and DNS settings as well as the IP address.
- If the computers are configured correctly, but still not working, check the Gateway. Ensure that it is connected and on. Connect to it and check its settings. (If you cannot connect to it, check the Ethernet and power connections.)

Problem: **Some applications do not run properly when using the Gateway.**

Solution: The Gateway processes the data passing through it, so it is not transparent.

- If you are running a supported Windows operating system, ensure that the UPnP feature is enabled.
- If this does not solve the problem or your operating system does not support UPnP you can use the *DMZ* function. This should work with almost every application, but:
  - It is a security risk, since the firewall is disabled for the DMZ computer.
  - Only one (1) computer can use this feature.
- A third option is to use the Firewall Snooze Control feature to temporarily disable the firewall to allow the application to function unimpeded.

Contacting Technical Support

Before contacting technical support, please refer to the previous troubleshooting information. For issues concerning DSL service or connectivity, contact your Internet Service Provider (ISP) directly. If you are still unable to resolve the problem, be prepared to provide the following information:

- Internet Service Provider and service type (DSL, cable)
- Product model number (SpeedStream SS6000 Series)
- Date of purchase or installation
- Description of problem

Technical Support services are available via the Internet, e-mail and telephone:

Telephone: (972) 852-1000
Fax: (972) 852-1001
Email: infor.ssn@siemens.com
Internet: http://www.icn.siemens.com/subscriber

Appendix B

Specifications

Media Interface:	RJ-11 DSL WAN connection (5) 10/100Base-T RJ-45 Ethernet LAN connections (Auto-MDI/MDI-X) USB Type B connection DB-9 RS-232 Serial console port
Diagnostic LEDs:	Power, Status, Link and Activity for DSL, Ethernet, USB (optional), and Wireless
Management:	Intuitive, Web-based management Comprehensive hardware diagnostics SNMPv1 support UPnP IGD-NAT traversal support XML Management Scheme, DSL Forum 2002-281
Security:	PAP (RFC 1334), CHAP (RFC 1994) Password Authentication Access Control list Stateful Inspection Firewall with Denial of Service (DoS) protection Pre-configured firewall levels for ease of use with “Custom” level for advanced users Filter on source and/or destination IP address Filter on transport protocol and/or port number Firewall logging with Network Time Protocol support and Syslog support DMZ support and Firewall “Snooze” feature Content filtering ICSA compliancy mode
Standards Compliance:	IEEE 802.1d, 802.11g, 802.3, and 802.3u USB 1.1 (optional) T1.413 issue 2 G.992.1 (G.DMT) G.992.2 (G.Lite)

Routing:	DHCP server and DNS agent Network Address Port Translation (NAPT) Network Address Translation (NAT) Packet filtering RFC 2364 Point-to-Point Protocol over ATM PVCs (PPPoA) RFC 2516 Point-to-Point Protocol over Ethernet (PPPoE) RFC 2684 (formerly 1483) Bridged Ethernet and routed encapsulation RFC 2225 (formerly 1577) Classical IP over ATM PPPoE Relay/Bridging Configurable PAP and CHAP authentication TCP/IP with RIP1 and RIP2 or static routing on the LAN and/or WAN Dynamic DNS Support IP QoS (depending on configuration)
Bridging:	IEEE 802.1.d Transparent Learning Bridge (dynamic learning of up to 255 addresses) RFC 2684 (formerly 1483) Bridged Ethernet over ATM PVCs Spanning Tree support
AAL and ATM Support:	Up to 8 active VCCs across VPI 0-255, VCI 0-65535 address range ATM Forum UNI3.1/4.0 PVC ATM Traffic class: UBR, CBR, VBRnrt, VBRrt OAM F5
Power:	12V power supply included 1000mA max. output
Certifications:	FCC Part 15, Class B FCC Part 68 UL Listed CE certification CSA Industry Canada WHQL

Siemens Subscriber Network
4849 Alpha Road
Dallas, TX 75244 USA
(972) 852-1000 Tel
(972) 852-1001 Fax
info.ssn@siemens.com
http://www.icn.siemens.com/subscriber